EXHIBIT A

Ciena's Technology Tutorial

4:17-cv-05920-JSW

Dr. Richard Gitlin

July 9, 2020

Richard Gitlin, Sc. D.

50+ years of communications and networking leadership

Education:

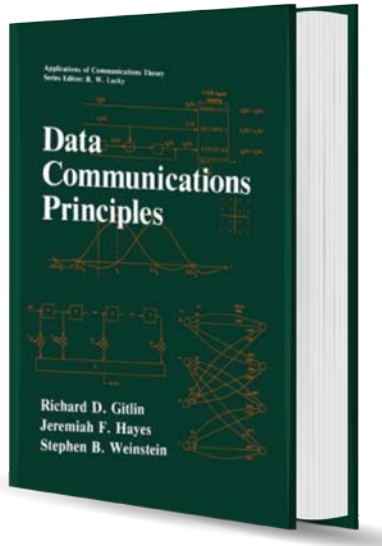
- Doctorate in Engineering Science from Columbia in 1969

Experience:

- 30+ years at Bell Labs (SVP at retirement)
- Visiting Professor at Columbia University
- CTO Silicon Valley Startup
- Distinguished University Professor at University of South Florida

Awards and Accomplishments:

- National Academy of Engineering
- Charter Fellow, National Academy of Inventors
- IEEE Fellow, Bell Labs Fellow
- Florida Inventors Hall of Fame
- Data communications textbook, 170 papers, 71 U.S. Patents

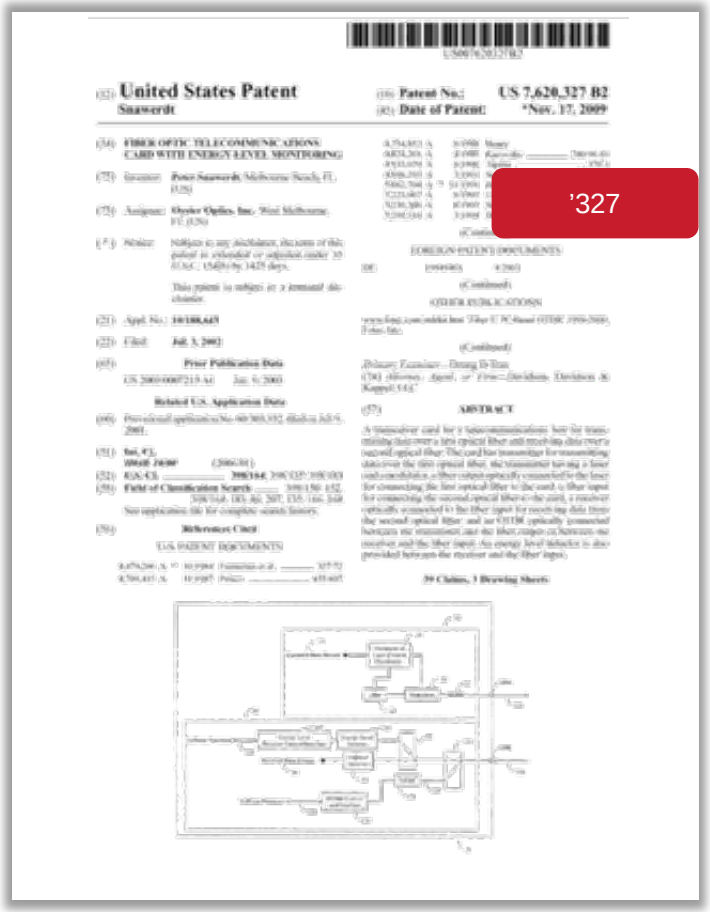


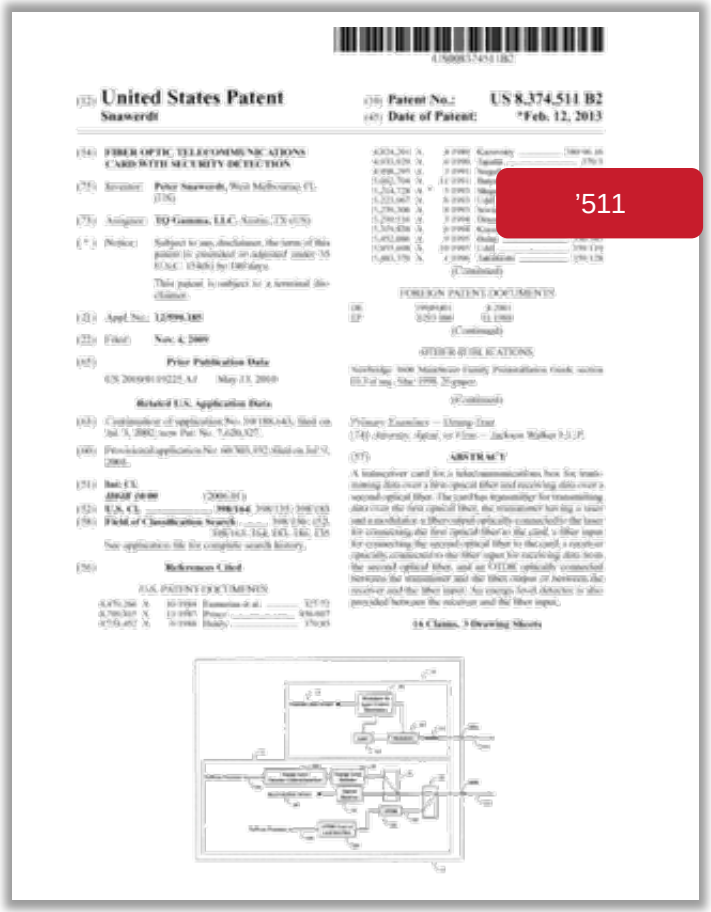
Major Innovations:

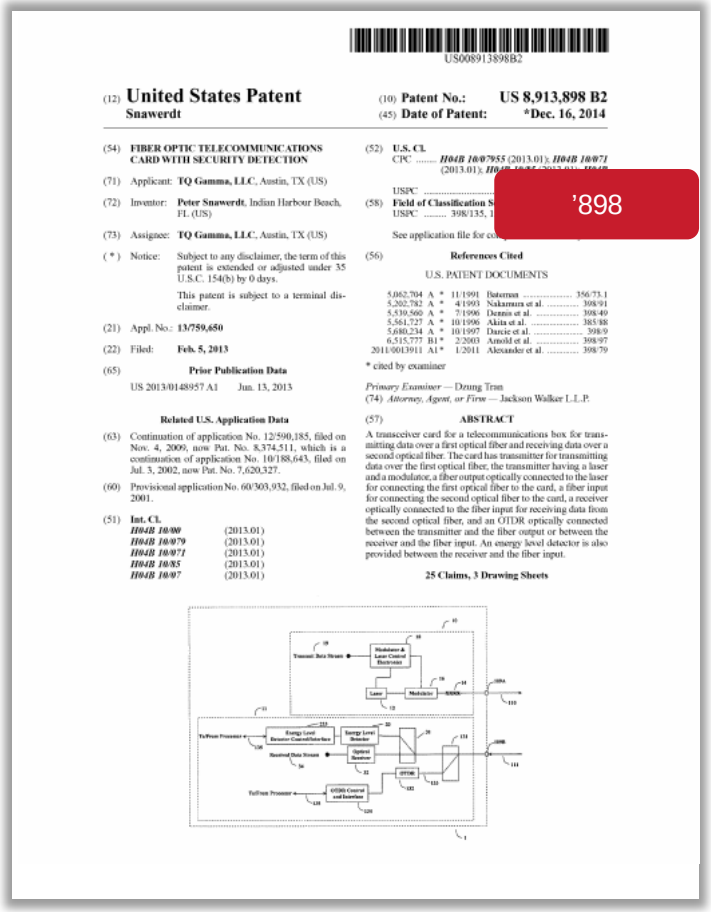
- Co-inventor of Digital Subscriber Line (DSL) technology
- Electro-optical receiver processing
- Smart antenna, MIMO wireless technology

Asserted Patents: U.S. Patent Nos. 7,620,327; 8,374,511; 8,913,898

FIBER OPTIC TELECOMMUNICATIONS CARD *WITH ENERGY LEVEL MONITORING*







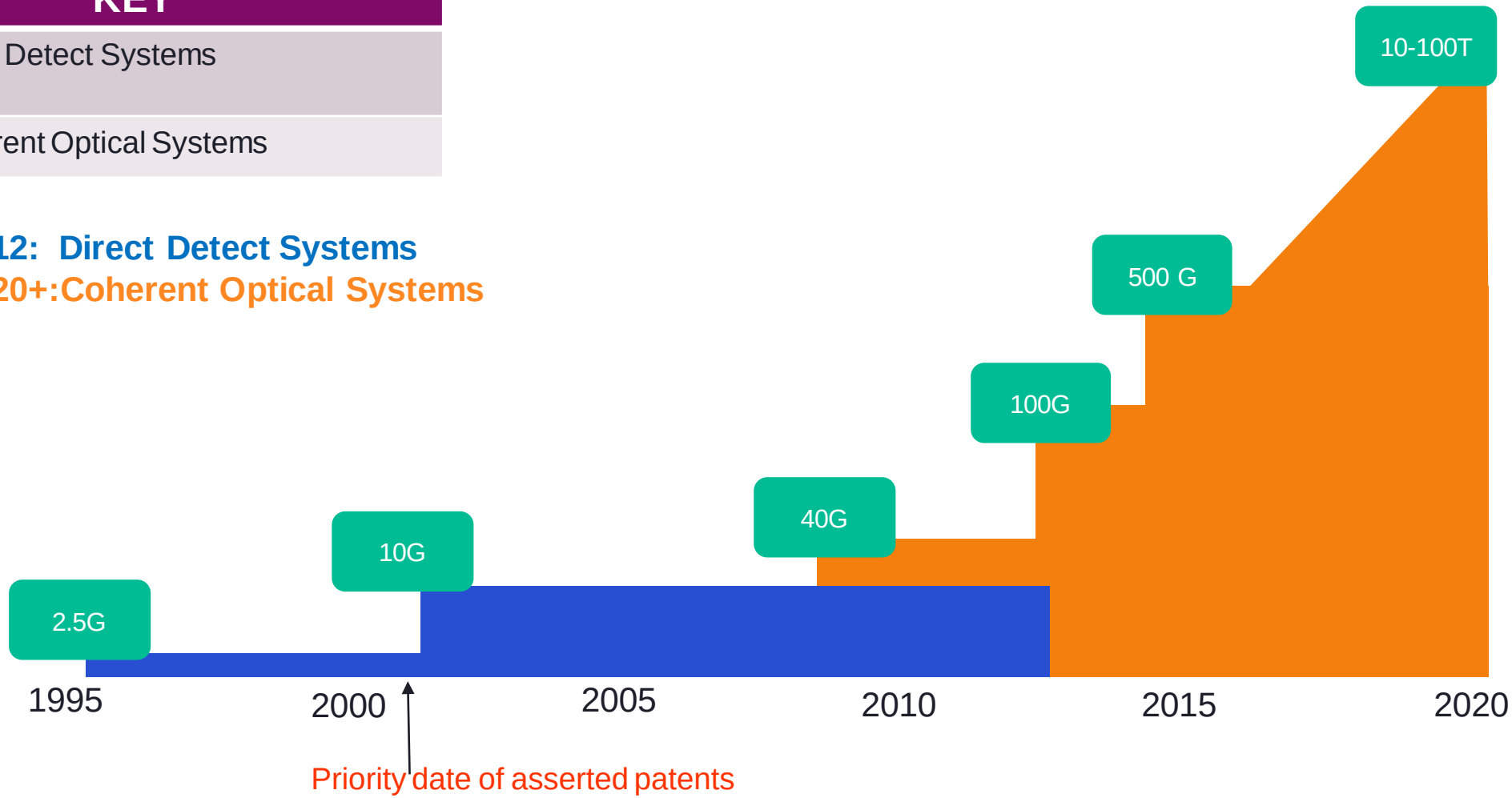
According to the common specification in the Asserted Patents, existing "systems have the disadvantage that the optical fiber can be easily tapped and are not secure," and the Asserted Patents describe the invention as "providing secure optical data transmission over optical fiber" by using tapping detection capabilities.

OVERVIEW OF OPTICAL COMMUNICATION SYSTEMS

Evolution of Fiber Optic Communication Systems

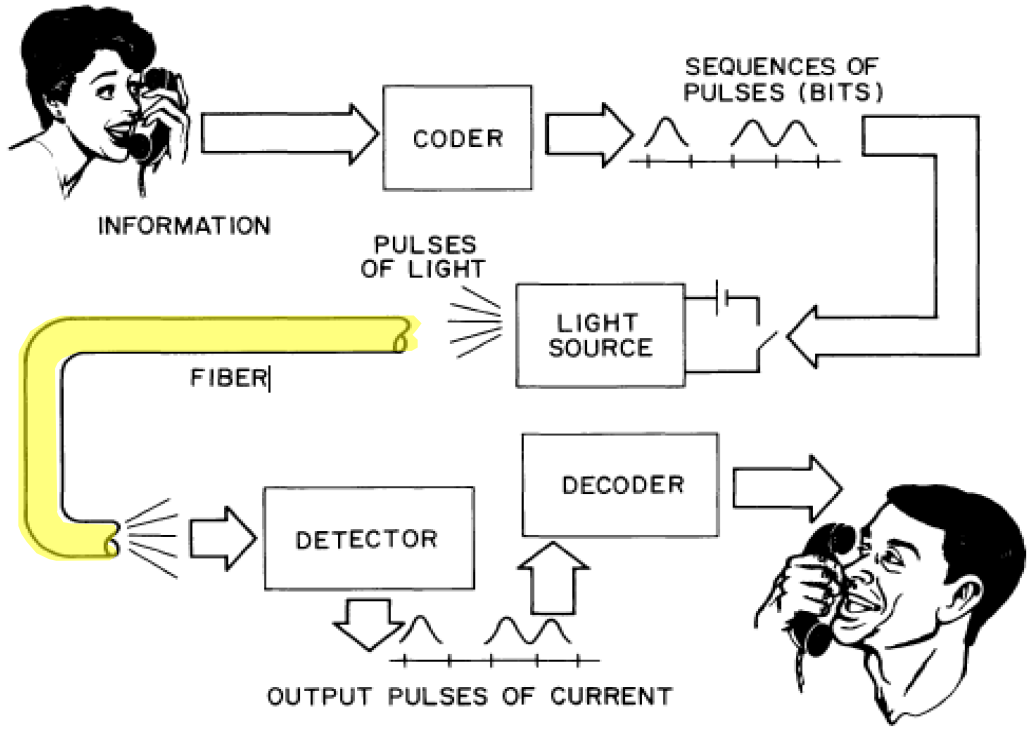
KEY
Direct Detect Systems
Coherent Optical Systems

1995~2012: Direct Detect Systems
2008~2020+:Coherent Optical Systems



G denotes gigabits (billion) per second

Exemplary Fiber Optics Voice Communications System

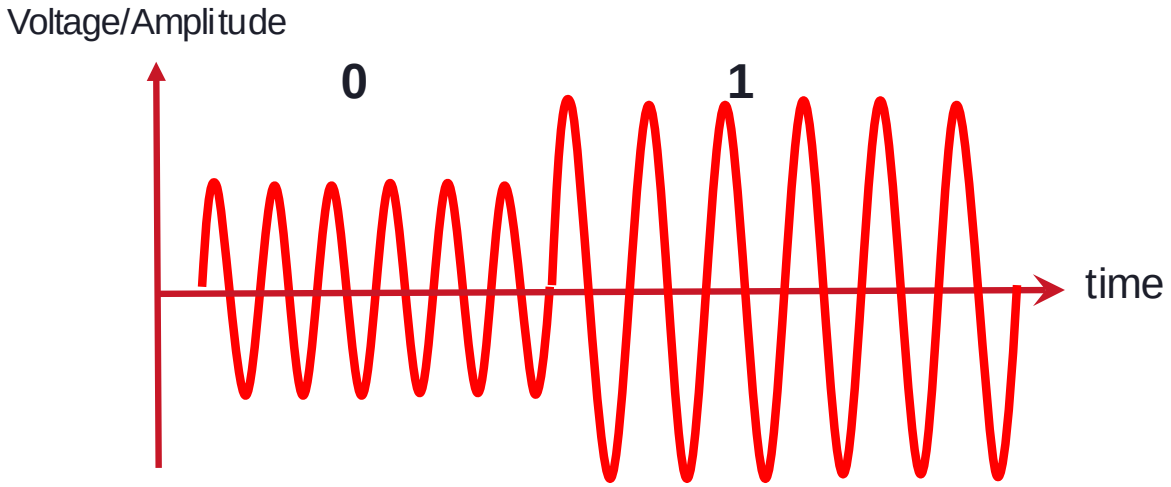


- Voice is digitized to binary data by the coder.
- The speech coder output bits that modulate the intensity of the optical light source (on/off).
- The modulated signal is transmitted over the fiber.
- At the receiver the intensity of the optical pulses is detected by a photodetector.
- The electrical output signal is applied to the speech decoder.

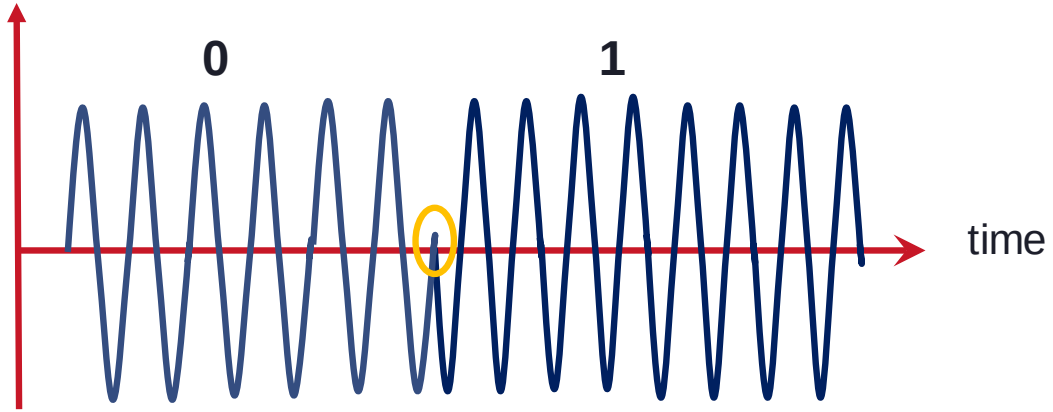
Optical Signal Basics - Modulation of an Optical Signal

Light travels in waves of very high frequencies. In order to transmit data over long distances using optical communications we manipulate, or modulate, carrier lightwaves to transport the data.

Amplitude Modulation (AM)

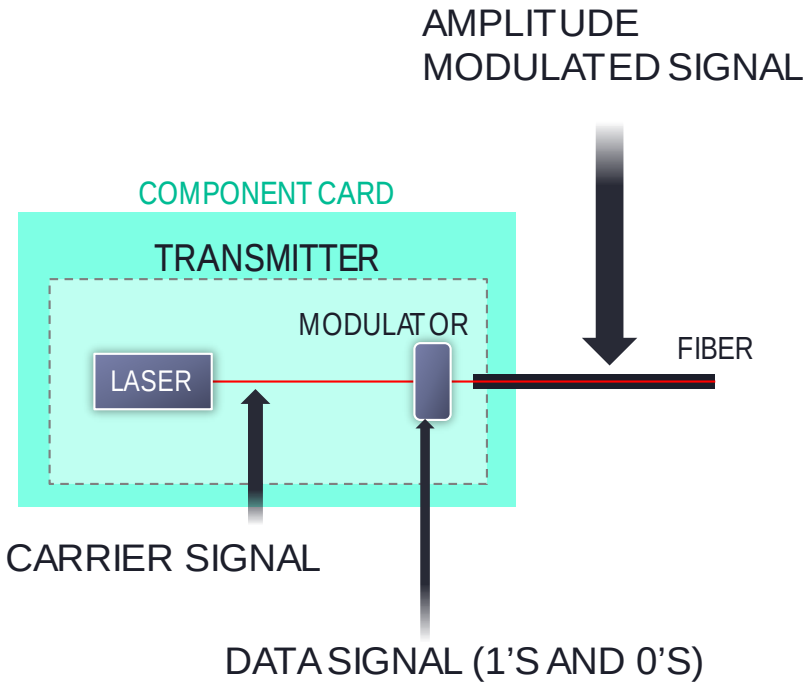


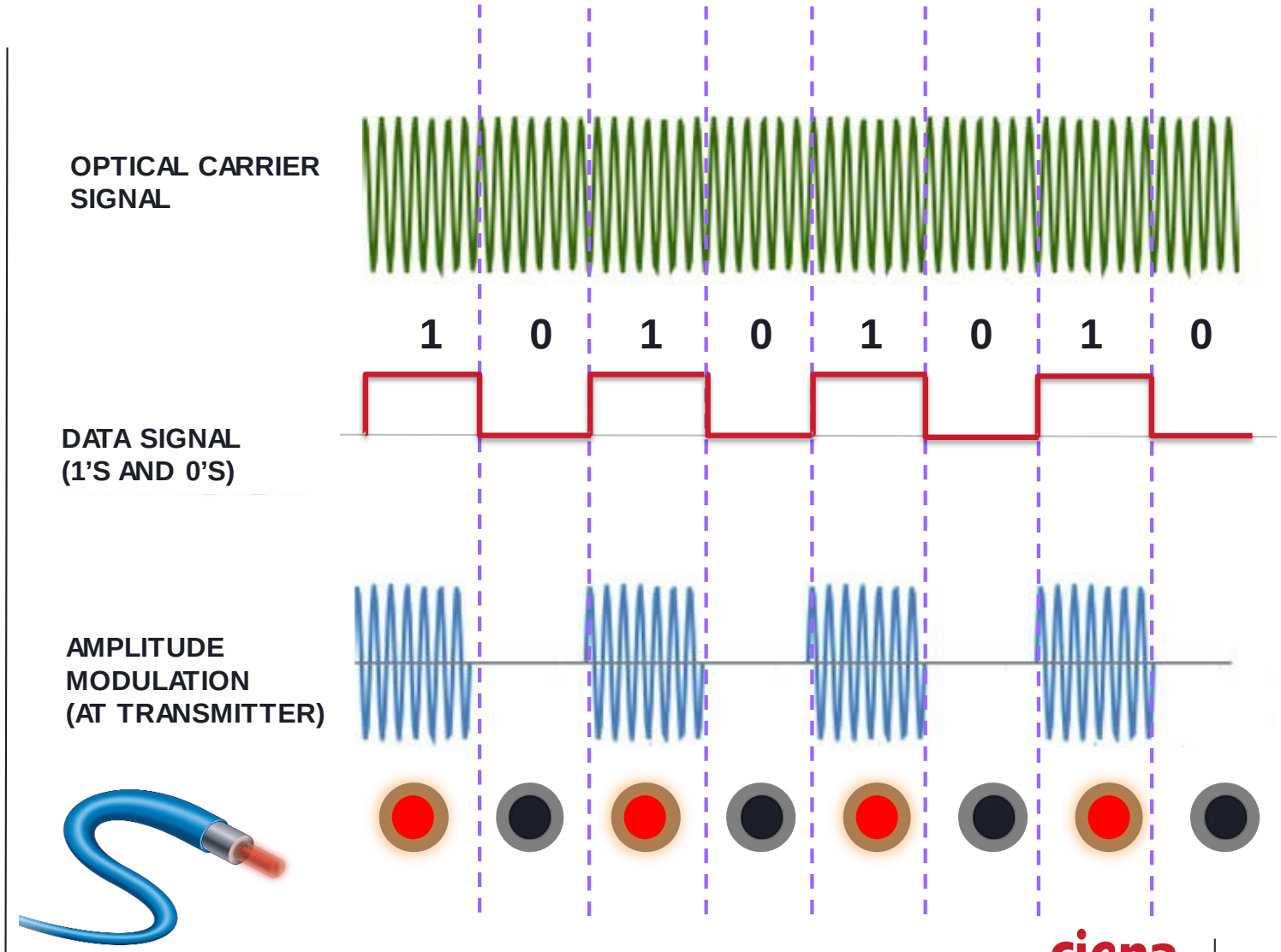
Phase Modulation (PM)



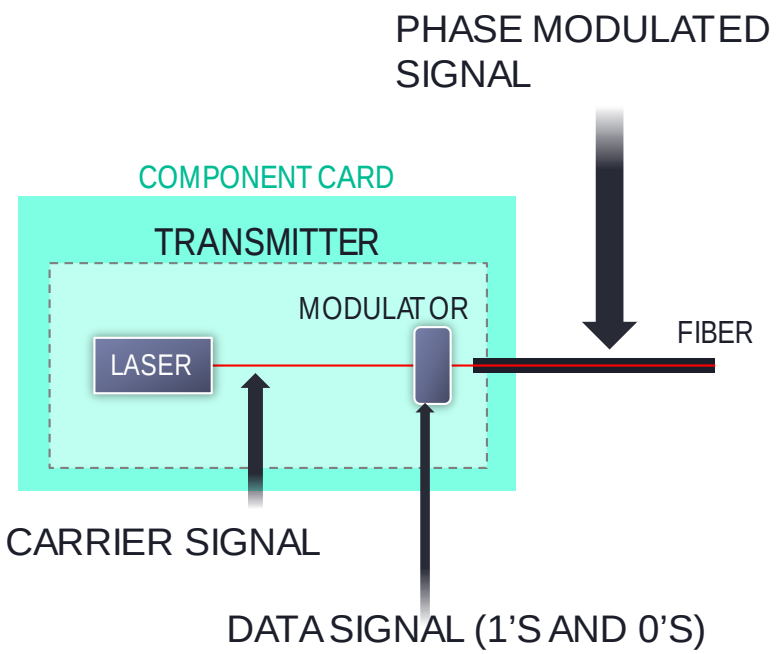
180° phase shift (= “1”)

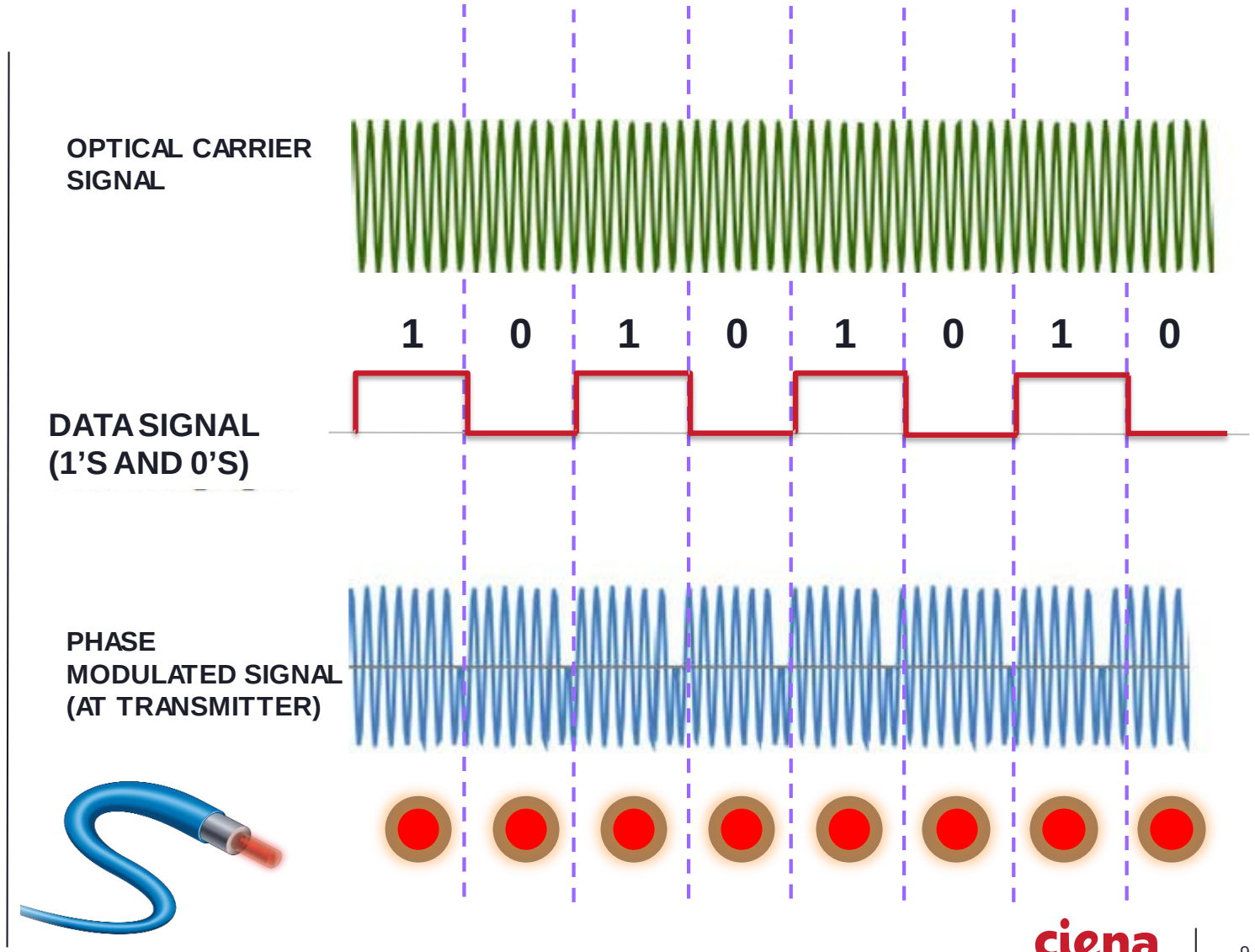
Amplitude Modulated (AM) Optical Signal





Phase Modulated (PM) Optical Signal



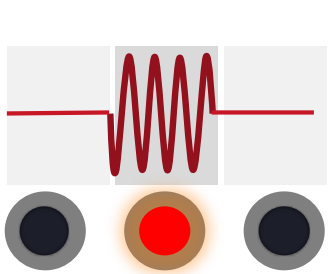


Receiver Processing

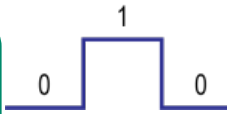
Amplitude Modulated Signals

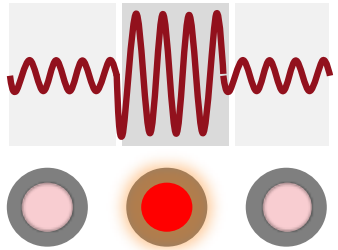
The receiver determines if a zero or a one is sent by looking at the ***intensity*** of the light.

The ***intensity*** is synonymous with the ***brightness*** of the light and is related to the light energy.

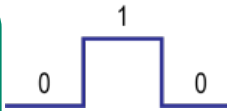


Receiver (OOK)





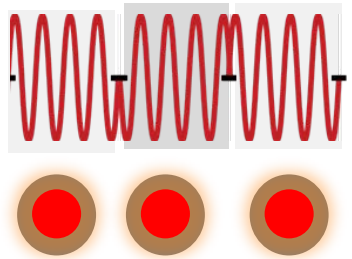
Receive (ASK)



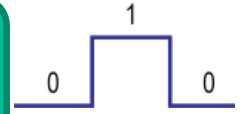
Phase Modulated Signals

The receiver determines if a zero or a one is sent by looking at the ***phase*** of the light.

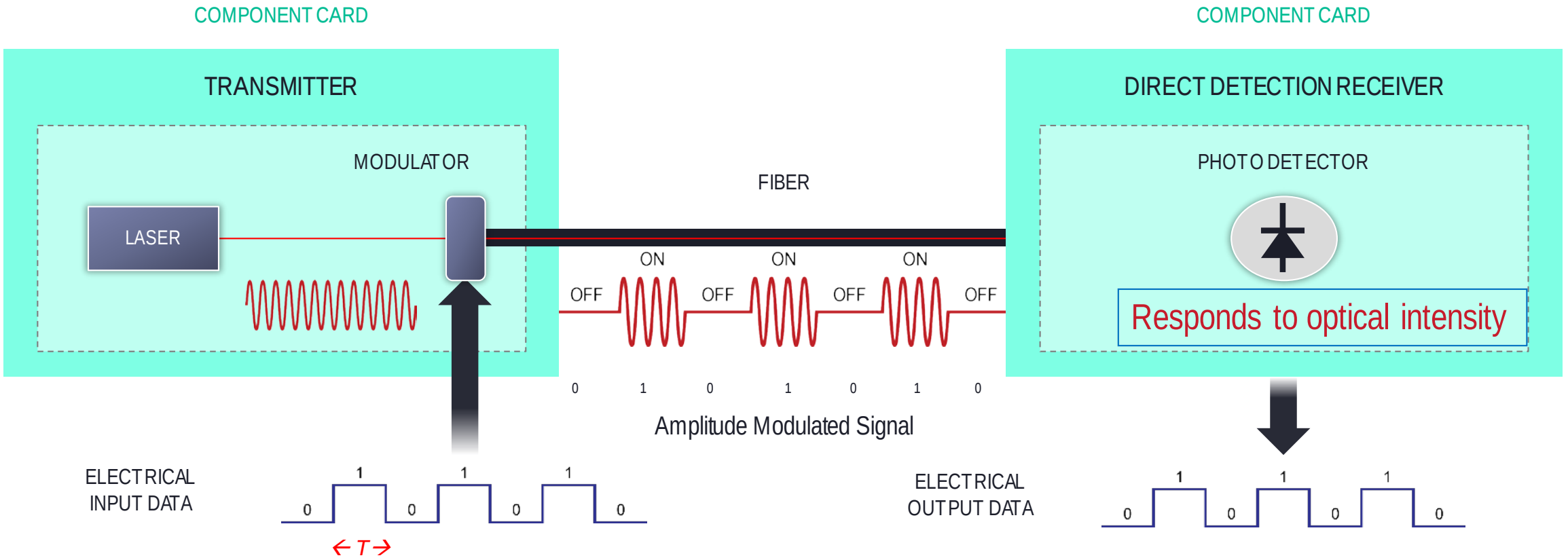
For this presentation, it will be assumed, as the patents do, that the ***brightness or amplitude*** of the received phase modulated signal remains ***constant***.



Receiver (PM)

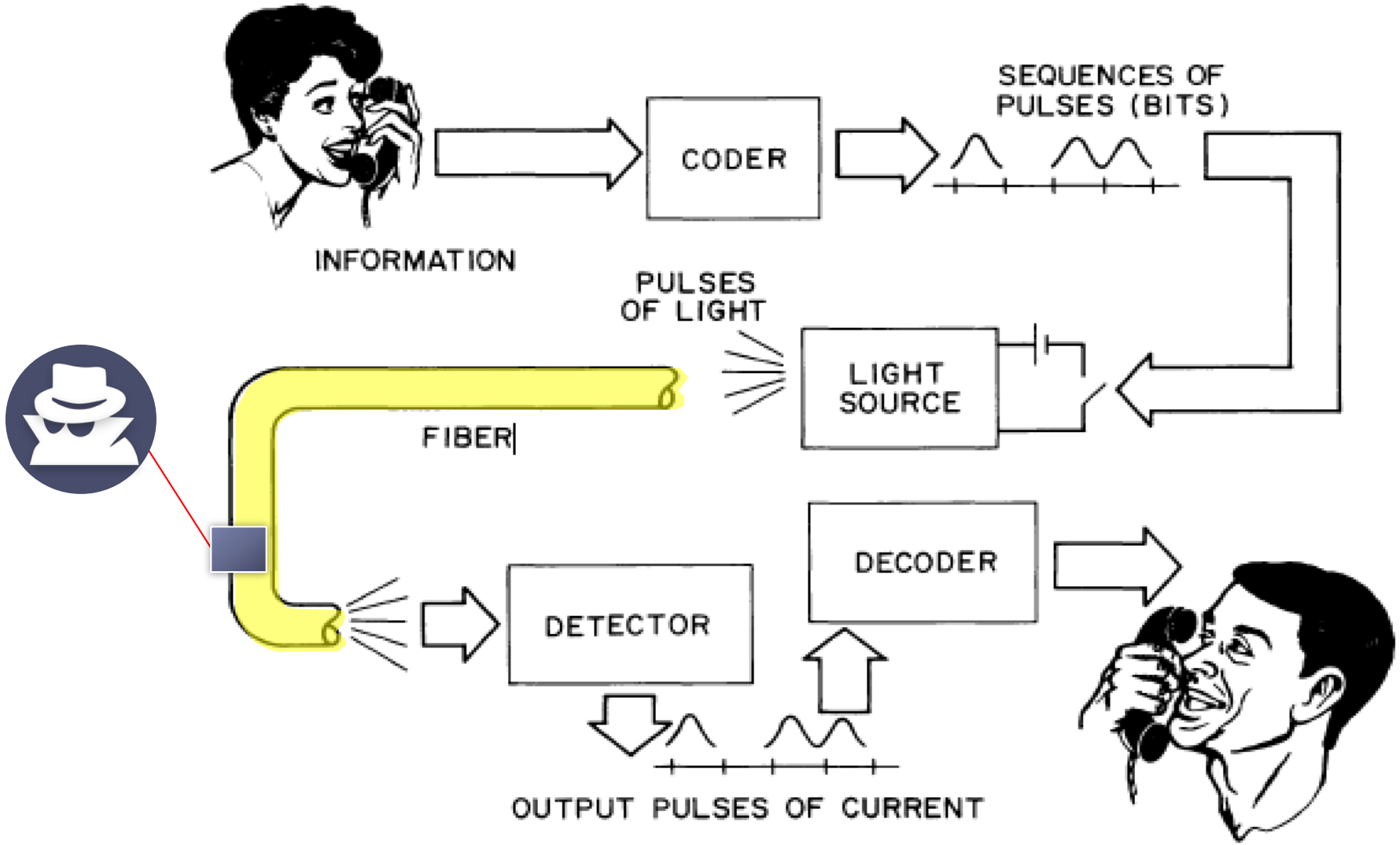


Early Fiber Optic Transmission Systems Used Amplitude Modulation and Direct Detection



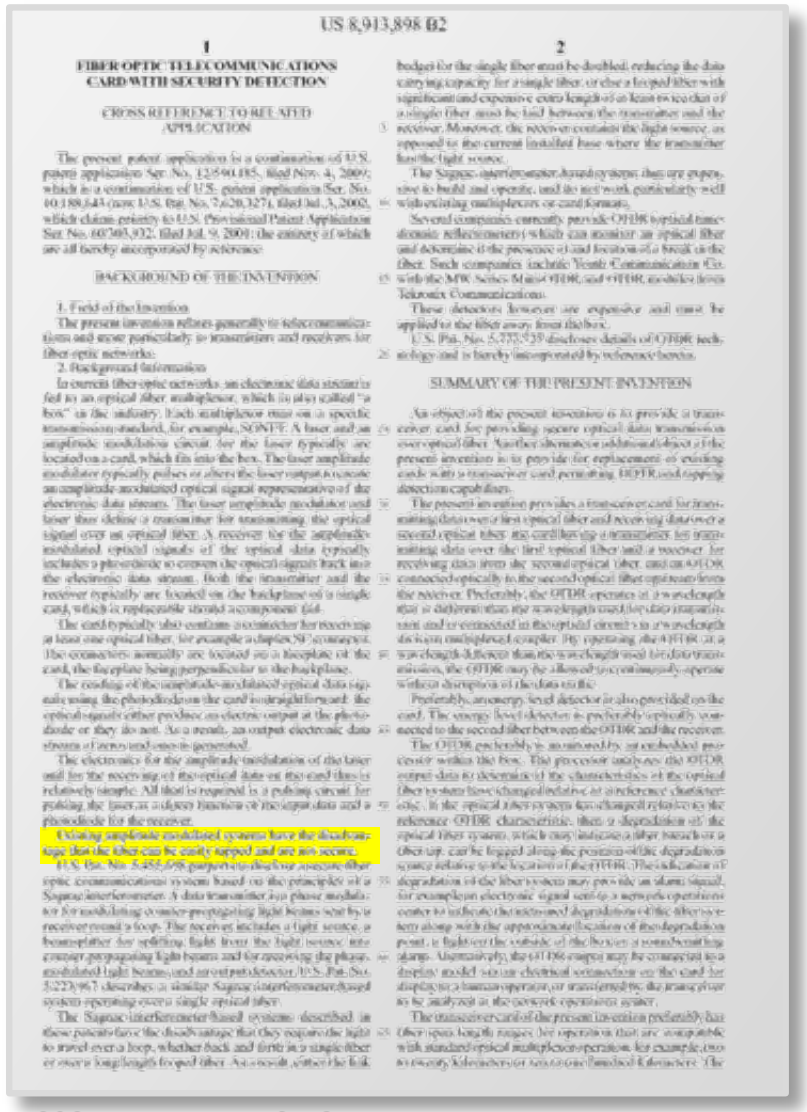
SYSTEM SECURITY AS PRESENTED IN PATENTS

Fiber Optic Systems Were Susceptible to Unwanted Tapping



The patents address a concern that a network intruder could tap the optical fiber without easily being detected

Security of Fiber Optic Cables



US 8,913,898 B2

1

FIBER OPTIC TELECOMMUNICATIONS CARD WITH SECURITY DETECTION

CROSS REFERENCE TO RELATED APPLICATION

The present patent application is a continuation of U.S. patent application Ser. No. 12/590,185, filed Nov. 4, 2009, which is a continuation of U.S. patent application Ser. No. 10/188,644 (now U.S. Pat. No. 7,620,327), filed Jul. 3, 2002, which claims priority to U.S. Provisional Patent Application Ser. No. 60/303,932, filed Jul. 9, 2001, the entirety of which are all hereby incorporated by reference.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates generally to telecommunications and more particularly to transmitters and receivers for fiber optic networks.

2. Background Information

In current fiber optic networks, an electronic data system is fed to an optical fiber multiplexer, which is also called "a box" in the industry. Each multiplexer runs on a specific transmission standard, for example, SONET. A laser and an amplitude modulation circuit for the laser typically are located on a card, which fits into the box. The laser amplitude modulator typically pulses or alters the laser output to create an amplitude modulated optical signal representative of the electronic data stream. The laser amplitude modulator and laser thus define a transmitter for transmitting the optical signal over an optical fiber. A receiver for the amplitude modulated optical signals of the optical data typically includes a photodiode to convert the optical signals back into the electronic data stream. Both the transmitter and the receiver typically are located on the backplane of a single card, which is replaceable should a component fail.

The card typically also contains a connector for receiving at least one optical fiber, for example a duplex SC connector. The connectors normally are located on a faceplate of the card, the faceplate being perpendicular to the backplane.

The reading of the amplitude-modulated optical data signals using the photodiode on the card is straightforward: the optical signals either produce an electric output at the photodiode or they do not. As a result, an output electronic data stream of zeros and ones is generated.

The electronics for the amplitude modulation of the laser and for the receiving of the optical data on the card thus is relatively simple. All that is required is a pulsing circuit for pulsing the laser as a digital function of the input data and a photodiode for the receiver.

Existing amplitude modulated systems have the disadvantage that the fiber can be easily tapped and are not secure.

U.S. Pat. No. 5,455,698 purports to disclose a secure fiber optic communications system based on the principles of a Sagnac interferometer. A data transmitter has phase modulator for modulating counter-propagating light beams sent by a receiver round a loop. The receiver includes a light source, a beamsplitter for splitting light from the light source into counter-propagating light beams and for receiving the phase-modulated light beams, and an output detector. U.S. Pat. No. 5,223,967 describes a similar Sagnac interferometer-based system operating over a single optical fiber.

The Sagnac interferometer-based systems described in these patents have the disadvantage that they require the light to travel over a loop, whether back and forth in a single fiber or over a long length looped fiber. As a result, either the link budget for the single fiber must be doubled, reducing the data carrying capacity for a single fiber, or else a looped fiber with significant and expensive extra length of at least twice that of a single fiber must be laid between the transmitter and the receiver. Moreover, the receiver contains the light source, as opposed to the current installed base where the transmitter has the light source.

The Sagnac interferometer-based systems thus are expensive to build and operate, and do not work particularly well with existing multiplexers or card formats.

Several companies currently provide OTDR (optical time domain reflectometer) which can monitor an optical fiber and determine if the presence of and location of a break in the fiber. Such companies include Yeonic Communication Co. with the MW Series Mini-OTDR, and OTDR modules from Tektronix Communications.

These detectors however are expensive and must be applied to the fiber away from the box.

U.S. Pat. No. 5,777,529 discloses details of OTDR technology and is hereby incorporated by reference herein.

SUMMARY OF THE PRESENT INVENTION

An object of the present invention is to provide a transceiver card for providing secure optical data transmission over optical fiber. Another alternative object of the present invention is to provide for replacement of existing cards with a transceiver card permitting OTDR and tapping detection capabilities.

The present invention provides a transceiver card for transmitting data over a first optical fiber and receiving data over a second optical fiber. The card has up a transmitter for transmitting data over the first optical fiber and a receiver for receiving data from the second optical fiber, and an OTDR connected optically to the second optical fiber upstream from the receiver. Preferably, the OTDR operates at a wavelength that is different than the wavelength used for data transmission and is connected to the optical circuit via a wavelength division multiplexer coupler. By operating the OTDR at a wavelength different than the wavelength used for data transmission, the OTDR may be allowed to continuously operate without disruption of the data on the

Preferably, an energy level detector is also provided on the card. The energy level detector is preferably optically connected to the second fiber between the OTDR and the receiver.

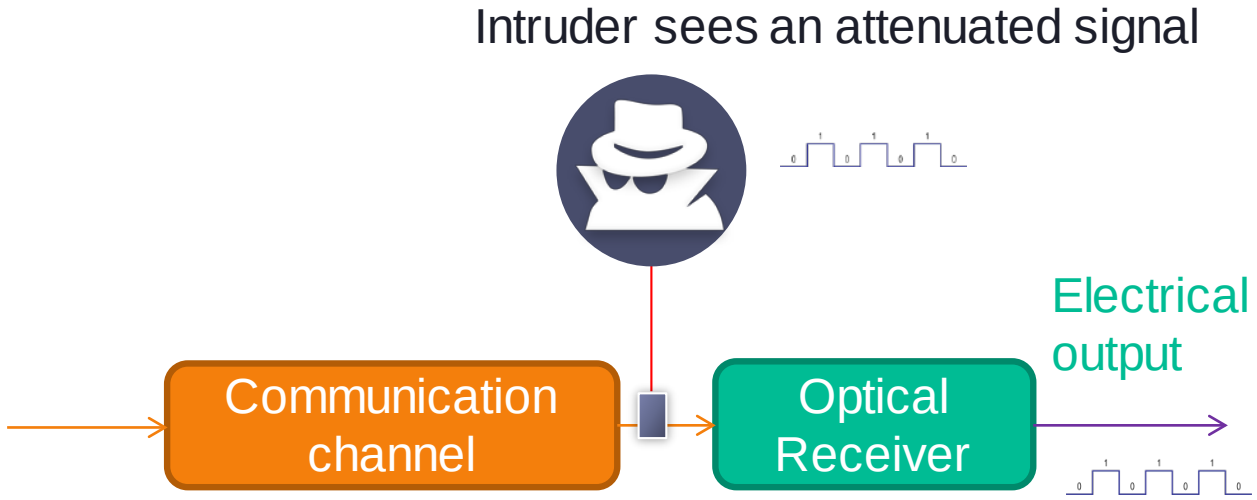
The OTDR preferably is monitored by an embedded processor within the box. The processor analyzes the OTDR output data to determine if the characteristics of the optical fiber system have changed relative to a reference characteristic, etc. In the optical fiber system has changed relative to the reference OTDR characteristic, then a degradation of the optical fiber system, which may indicate a fiber breach or a fiber tap, can be logged along the presence of the degradation relative to the location of the OTDR. The indication of degradation of the fiber system may provide an alarm signal, for example an electronic signal sent to a remote operations center to indicate the detected degradation of the fiber system along with the approximate location of the degradation point, a light over the outside of the box on a control/alarm lamp. Alternatively, the OTDR output may be connected to a display, model via an electrical connection on the card for displaying to human operator, or transmitted by the transceiver to be analyzed at the control operations center.

The transceiver card of the present invention preferably has fiber optic length ranges for operation that are compatible with standard optical multiplexer operation, for example, up to twenty kilometers or less over standard fiber. The

'898 patent at 1:52-53

> Existing amplitude modulated systems have the disadvantage that the fiber can be easily tapped and are not secure.

'898 patent at 1:52-53



How is optical tapping performed?

What Is An Optical Tap?

OYSTER OPTICS, Inc.

Securing Fiber Optic Communications against Optical Tapping Methods

Optical tapping devices placed in public and private optical networks today allow unfettered access to all communications and information transiting any fiber segment. Available legally and inexpensively from numerous manufacturers worldwide, optical taps are standard network maintenance equipment that are in use daily. When used nefariously, optical taps provide an excellent method of intercepting voice and data communications with virtually no chance of being detected. Intruders are therefore rewarded with a bounty of relevant information while subject to a very low risk of being caught. Optical network equipment manufacturers do not currently incorporate adequate protection and detection technologies in their platforms to monitor such network breaches in real-time. Network operators thus cannot safeguard the optical signals on their networks and therefore cannot prevent the extraction of sensitive data and communications. Government networks, while assuredly more secure, are also vulnerable to certain types of advanced passive and active tapping methods. This background paper serves to provide an overview of the vulnerabilities of today's modern optical networks; describe methods of addressing such issues; and introduce Oyster Optics' patented optical security, monitoring, intrusion detection and breach localization solutions.

INTRODUCTION

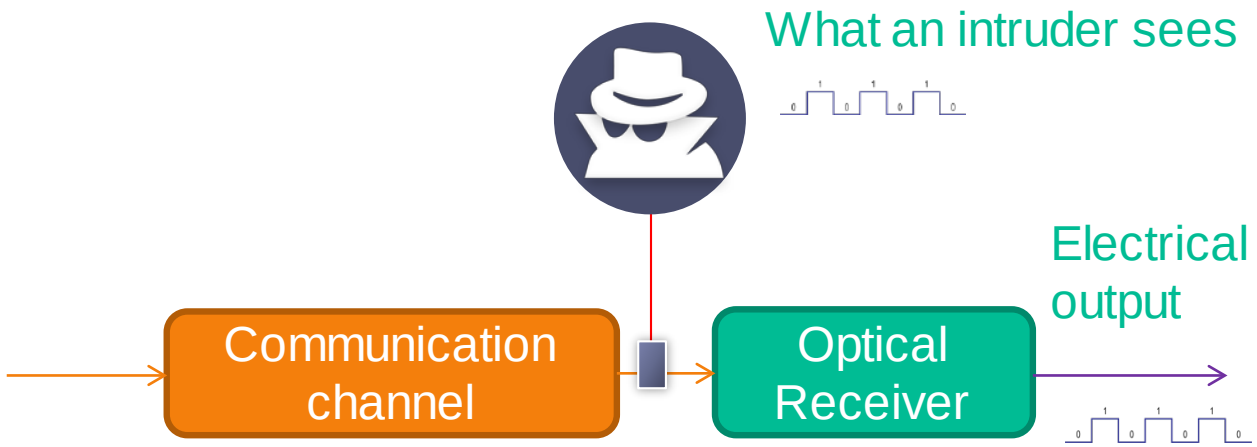
Fiber optic telecommunications systems make up the backbone of all modern communications networks. Whether voice, data, video, fax, wireless, email, TV or otherwise, over 180 million miles of fiber optic cables worldwide transport the ever-increasing majority of our diverse information and communications. Modern economies and societies rely on the availability, confidentiality and integrity of critical fiber optic network infrastructures to function properly and efficiently.

With the initial introduction of fiber optic telecommunications systems came the belief that fiber-based transmissions are inherently secure. It has since been proven that not only are fiber optic systems simple to tap, but in many respects they are simpler to tap than their copper-based predecessors. Furthermore, tapped optical networks divulge much greater pertinent information in a more orderly and digitized manner. In fact, many fiber optic taps are standard network maintenance equipment used daily by carriers worldwide. Used illicitly, however, such devices *allow the extraction of all voice and data communications in the fiber plant with little or no chance of detection.*

This is achieved because the light within the cable contains all the information in the transmitted signal and can be easily captured, interpreted and manipulated with standard off-the-shelf tapping equipment. Private and public networks today do not incorporate methods for detecting optical taps in real-time, offering an intruder a relatively safe data extraction proposition. As fiber optic systems transmit large volumes of data as light within an optical fiber, such methods are thus a preferred low-risk method of intelligence gathering, reaping access to large amounts of information. From an eavesdropping and espionage point-of-view the benefits are obvious.

Today we live in a society where corporate espionage has become an international sport. As communications using fiber optics become increasingly ubiquitous, so too does the potential for the illegal tapping and

Dkt. No. 100-3; Ex. M (Oyster Optics White Paper)



Optical tapping "devices *allow the extraction of all voice and data communications in the fiber plant with little or no chance of detection.*

This is achieved because the light within the cable contains all the information in the transmitted signal and can be easily captured, interpreted and manipulated with standard off-the-shelf tapping equipment."

Dkt. No. 100-3; Ex. M (Oyster Optics White Paper) at 1

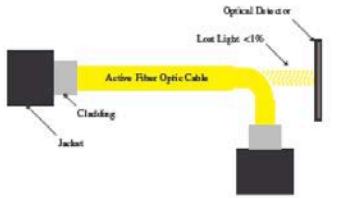
Examples of Optical Taps

- Splice
- Splitter or Coupler (Variable)
- Non-touching methods (passive and active)

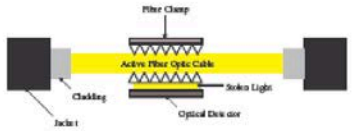
SPLICE: The simplest method of tapping is by splicing the optical fiber briefly and inserting equipment to allow for the signal to transit to the end party while also being intercepted by the intruder. Optical splices do provide a momentary lapse of data while the fiber is not operational. Carriers do not, however, have the real-time ability to locate fiber breaks and must then usually roll-out trucks, technicians and insert additional external equipment. Thus, if downtime is short, many operators will attribute the disturbance to a network glitch and allow data transit to continue, unaware that a tap has been placed. Most off-the-shelf tapping equipment today, however, does not interrupt the signal and thus the splicing method is not preferred.

SPLITTERS AND COUPLERS (VARIABLE): Such methods allow the tapping of an optical fiber without actually breaking the fiber or disrupting the data flow. One of the lesser-known properties of optical fibers is that light is easily lost from both the jacket and the cladding of the fiber, particularly if the fiber is bent, or clamped, in such a way that micro-bends or ripples are formed in its surface. Perhaps the simplest example of such phenomena is that one is able to see the light in an optical fiber if one holds an optical fiber in one's hands. Just as simply as one sees the light (as one's eyes are after all biological optical detectors), so does the equipment designed to interpret it. In reality, all that is required to extract all of the information traveling through an optical fiber is to introduce a slight bend into the fiber, or clamp onto it at any point along its length, and photons of light will leak into the receiver of the intruder.

Diagram 2: Illustrated below are two simple taps that allow for the bleeding of light from the optical fiber.



2(a)

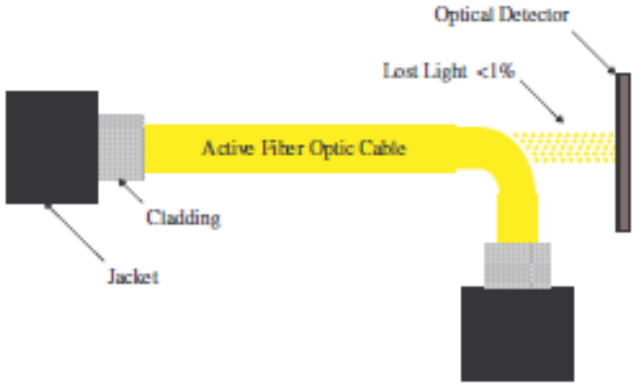


2(b)

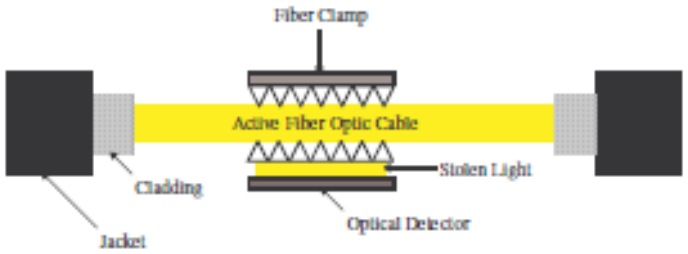
In fact, many optical fiber test instruments are designed specifically to take advantage of this fact. For example, below is a commonly available Optical Fiber Identifier that is used to determine the direction of an optical signal, without the need to remove the jacket. Other passive, non-intrusive tapping devices are also shown.

Dkt. No. 100-3; Ex. M (Oyster Optics White Paper)

Diagram 2: Illustrated below are two simple taps that allow for the bleeding of light from the optical fiber.



2(a)



2(b)

Dkt. No. 100-3; Ex. M at 4.

There are three primary methods for optical taps:

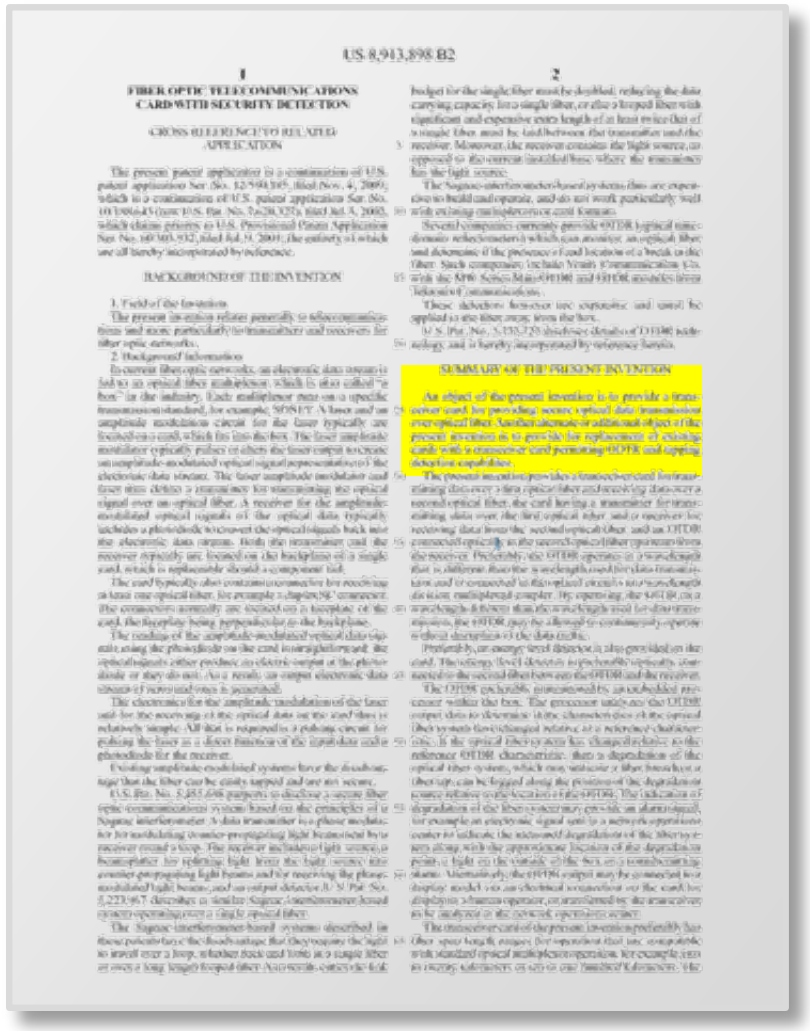
1) Splice (data loss)
2) Macro-bend, micro-bend, variable couplers (light loss)
3) Non-touching methods based on scattering (passive active)

Ex. M at 3-4

All of these tapping devices ***draw some of the light's power*** from the fiber optic line.

Why did the problem of undetectable tapping exist and how do the asserted patents claim to have solved the problem?

The Patentee Recognized a Need for Secure Optical Data Transfer that Required Tapping Detection Capabilities



US 8,913,898 B2

FIBER OPTIC TELECOMMUNICATIONS CARD WITH SECURITY DETECTION

SUMMARY OF THE PRESENT INVENTION

An object of the present invention is to provide a transceiver card for providing secure optical data transmission over optical fiber. Another alternate or additional object of the present invention is to provide for replacement of existing cards with a transceiver card permitting ODTR and tapping detection capabilites.

’898 patent at 2:24-29

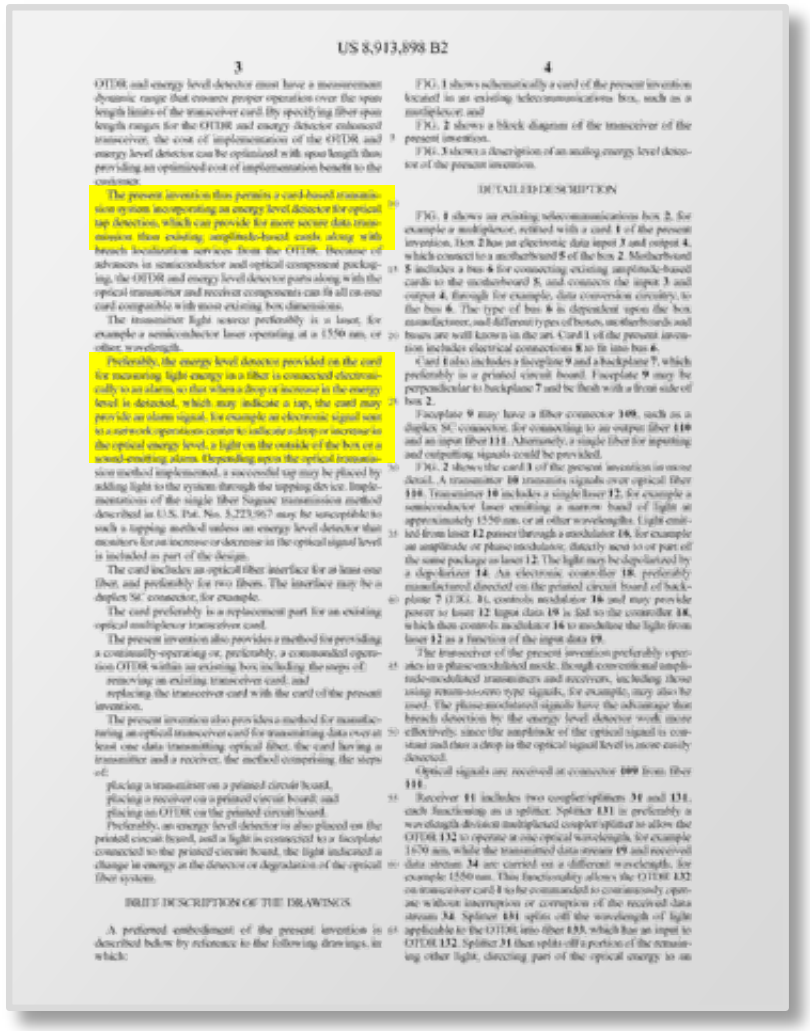
SUMMARY OF THE PRESENT INVENTION

An object of the present invention is to provide a transceiver card for providing secure optical data transmission over optical fiber. Another alternate or additional object of the present invention is to provide for replacement of existing cards with a transceiver card permitting ODTR and tapping detection capabilites.

’898 patent at 2:24-29

- Networks were not secure against tappers
- Need for ability to detect when a fiber optic line was tapped

More Secure Than "Amplitude-Based Cards" By Detecting A "Drop or Increase In the Energy Level" -- Required Constant Energy at Receiver



US 8,913,898 B2

3 4

OTDR and energy level detector must have a measurement dynamic range that ensures proper operation over the span length limits of the transceiver card. By specifying fiber span length ranges for the OTDR and energy detector enhanced transceiver, the cost of implementation of the OTDR and energy level detector can be optimized with span length thus providing an optimized cost of implementation benefit to the customer.

The present invention thus permits a card-based transmission system incorporating an energy level detector for optical tap detection, which can provide for more secure data transmission than existing amplitude-based cards along with breach localization services from the OTDR. Because of advances in semiconductor and optical component packaging, the OTDR and energy level detector parts along with the optical transmitter and receiver components can fit all on one card compatible with most existing box dimensions.

The transmitter light source preferably is a laser, for example a semiconductor laser operating at a 1550 nm, or other, wavelength.

Preferably, the energy level detector provided on the card for measuring light energy in a fiber is connected electronically to an alarm, so that when a drop or increase in the energy level is detected, which may indicate a tap, the card may provide an alarm signal, for example an electronic signal sent to a network operations center to indicate a drop or increase in the optical energy level, a light on the outside of the box or a sound-emitting alarm. Depending upon the optical transmission method implemented, a successful tap may be placed by adding light to the system through the tapping device. Implementations of the single fiber Sagnac transmission method described in U.S. Pat. No. 5,223,967 may be susceptible to such a tapping method unless an energy level detector that monitors for an increase or decrease in the optical signal level is included as part of the design.

The card includes an optical fiber interface for at least one fiber, and preferably for two fibers. The interface may be a duplex SC connector, for example.

The card preferably is a replacement part for an existing optical multiplexer transceiver card.

The present invention also provides a method for providing a continually-operating or, preferably, a commanded operation OTDR within an existing box including the steps of:

removing an existing transceiver card; and

replacing the transceiver card with the card of the present invention.

The present invention also provides a method for manufacturing an optical transceiver card for transmitting data over at least one data transmitting optical fiber, the card having a transmitter and a receiver, the method comprising the steps of:

placing a transmitter on a printed circuit board;

placing a receiver on a printed circuit board; and

placing an OTDR on the printed circuit board.

Preferably, an energy level detector is also placed on the printed circuit board, and a light is connected to a faceplate connected to the printed circuit board, the light indicated a change in energy at the detector or degradation of the optical fiber system.

BRIEF DESCRIPTION OF THE DRAWINGS

A preferred embodiment of the present invention is described below by reference to the following drawings, in which:

FIG. 1 shows schematically a card of the present invention located in an existing telecommunications box, such as a multiplexer; and

FIG. 2 shows a block diagram of the transceiver of the present invention.

FIG. 3 shows a description of an analog energy level detector of the present invention.

DETAILED DESCRIPTION

FIG. 1 shows an existing telecommunications box 2, for example a multiplexer, refitted with a card 1 of the present invention. Box 2 has an electronic data input 3 and output 4, which connect to a motherboard 5 of the box 2. Motherboard 5 includes a bus 6 for connecting existing amplitude-based cards to the motherboard 5, and connects the input 3 and output 4, through for example, data conversion circuitry, to the bus 6. The type of bus 6 is dependent upon the box manufacturer, and different types of buses, motherboards and boxes are well known in the art. Card 1 of the present invention includes electrical connections 8 to fit into bus 6.

Card 1 also includes a faceplate 9 and a backplane 7, which preferably is a printed circuit board. Faceplate 9 may be perpendicular to backplane 7 and be flush with a front side of box 2.

Faceplate 9 may have a fiber connector 109, such as a duplex SC connector, for connecting to an output fiber 110 and an input fiber 111. Alternately, a single fiber for inputting and outputting signals could be provided.

FIG. 2 shows the card 1 of the present invention in more detail. A transmitter 10 transmits signals over optical fiber 110. Transmitter 10 includes a single laser 12, for example a semiconductor laser emitting a narrow band of light at approximately 1550 nm, or at other wavelengths. Light emitted from laser 12 passes through a modulator 16, for example an amplitude or phase modulator, directly next to or part of the same package as laser 12. The light may be depolarized by a depolarizer 14. An electronic controller 18, preferably manufactured directed on the printed circuit board of backplane 7 (FIG. 1), controls modulator 16 and may provide power to laser 12 input data 19 is fed to the controller 18, which then controls modulator 16 to modulate the light from laser 12 as a function of the input data 19.

The transceiver of the present invention preferably operates in a phase-modulated mode, though conventional amplitude-modulated transmitters and receivers, including those using return-to-zero type signals, for example, may also be used. The phase-modulated signals have the advantage that breach detection by the energy level detector work more effectively, since the amplitude of the optical signal is constant and then a drop in the optical signal level is more easily detected.

Optical signals are received at connector 109 from fiber 111.

Receiver 11 includes two coupler/splitters 31 and 131, each functioning as a splitter. Splitter 131 is preferably a wavelength division multiplexed coupler/splitter to allow the OTDR 132 to operate at one optical wavelength, for example 1670 nm, while the transmitted data stream 19 and received data stream 34 are carried on a different wavelength, for example 1550 nm. This functionality allows the OTDR 132 on transceiver card 1 to be commanded to continuously operate without interruption or corruption of the received data stream 34. Splitter 131 splits off the wavelength of light applicable to the OTDR into fiber 133, which has an input to OTDR 132. Splitter 31 then splits off a portion of the remaining other light, directing part of the optical energy to an

'898 patent at 3:10-14; 3:22-29

> The present invention thus permits a card-based transmission system incorporating an energy level detector for optical tap detection, which can provide for more secure data transmission than existing amplitude-based cards along with breach localization services from the OTDR. Because of

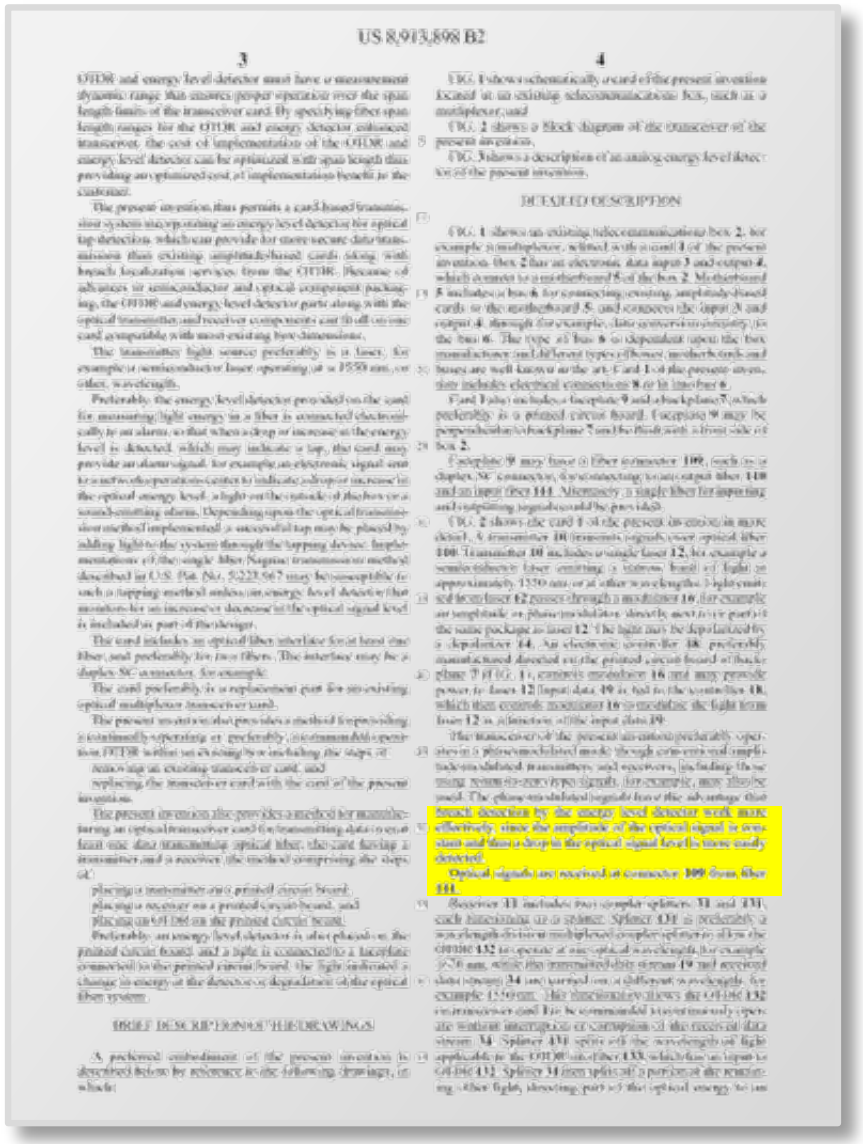
'898 patent at 3:10-14;

> Preferably, the energy level detector provided on the card for measuring light energy in a fiber is connected electronically to an alarm, so that when a drop or increase in the energy level is detected, which may indicate a tap, the card may provide an alarm signal, for example an electronic signal sent to a network operations center to indicate a drop or increase in the optical energy level, a light on the outside of the box or a sound-emitting alarm. Depending upon the optical transmis-

'898 patent at 3:22-29;

What was Oyster's preferred method for constant receiver energy?

Advantage of Phase-Modulated Signals Per Patent Disclosure



US 8,913,898 B2

3 4

OTDR and energy level detector must have a measurement dynamic range that ensures proper operation over the span length limits of the transceiver card. By specifying fiber span length ranges for the OTDR and energy detector enhanced transceiver, the cost of implementation of the OTDR and energy level detector can be optimized with span length thus providing an optimized cost of implementation benefit to the customer.

The present invention thus permits a card-based transmission system incorporating an energy level detector for optical tap detection, which can provide for more secure data transmission than existing amplitude-based cards, along with breach localization services from the OTDR. Because of advances in semiconductor and optical component packaging, the OTDR and energy level detector parts along with the optical transmitter and receiver components can fit all on one card compatible with most existing bore dimensions.

The transmitter light source preferably is a laser, for example a semiconductor laser operating at a 1550 nm, or other, wavelength.

Preferably, the energy level detector provided on the card for measuring light energy in a fiber is connected electronically to an alarm, so that when a drop or increase in the energy level is detected, which may indicate a tap, the card may provide an alarm signal, for example an electronic signal sent to a network operations center to indicate a drop or increase in the optical energy level. A light on the outside of the box or a sound-emitting alarm. Depending upon the optical transmission method implemented, a successful tap may be placed by adding light to the system through the tapping device. Implementations of the single fiber Nagata transmission method described in U.S. Pat. No. 5,223,967 may be susceptible to such a tapping method unless an energy level detector that monitors for an increase or decrease in the optical signal level is included as part of the design.

The card includes an optical fiber interface for at least one fiber, and preferably for two fibers. The interface may be a duplex SC connector, for example.

The card preferably is a replacement part for an existing optical multiplexer transceiver card.

The present invention also provides a method for providing a continuously operating or preferably non-disruptive operation OTDR within an existing box including the steps of:

removing an existing transceiver card; and

replacing the transceiver card with the card of the present invention.

The present invention also provides a method for manufacturing an optical transceiver card for transmitting data over at least one data transmitting optical fiber, the card having a transmitter and a receiver, the method comprising the steps of:

placing a transmitter on a printed circuit board;

placing a receiver on a printed circuit board; and

placing an OTDR on the printed circuit board.

Preferably, an energy level detector is also placed on the printed circuit board, and a light is connected to a faceplate connected to the printed circuit board, the light indicating a change in energy at the detector or degradation of the optical fiber system.

BRIEF DESCRIPTION OF THE DRAWINGS

A preferred embodiment of the present invention is described below by reference to the following drawings, in which:

DG. 1 shows schematically a card of the present invention located in an existing telecommunications box, such as a multiplexer; and

DG. 2 shows a block diagram of the transceiver of the present invention.

DG. 3 shows a description of an analog energy level detector of the present invention.

DETAILED DESCRIPTION

DG. 1 shows an existing telecommunications box 2, for example a multiplexer, without a card 1 of the present invention. Box 2 has an electronic data input 3 and output 4, which connect to a motherboard 5 of the box 2. Motherboard 5 includes a bus 6 for connecting existing, amplitude-based cards to the motherboard 5 and connects the input 3 and output 4 through, for example, data converters or circuitry in the bus 6. The type of bus 6 is dependent upon the box manufacturer and different types of buses, motherboards and buses are well known in the art. Card 1 of the present invention includes electrical connectors 8 or 8' to interface 6.

Card 1 also includes a faceplate 9 and a backplane 7, which preferably is a printed circuit board. Faceplate 9 may be perpendicular to backplane 7 and be fixed with a front side of box 2.

Faceplate 9 may have a fiber connector 100, such as a duplex SC connector, for connecting to an output fiber 110 and an input fiber 111. Alternately, a single fiber for inputting and outputting signals could be provided.

DG. 2 shows the card 1 of the present invention in more detail. A transmitter 10 transmits signals over optical fiber 100. Transmitter 10 includes a single laser 12, for example a semiconductor laser emitting a narrow band of light at approximately 1550 nm or at other wavelengths. Light emitted from laser 12 passes through a modulator 16, for example an amplitude or phase modulator, directly next to or part of the same package as laser 12. The light may be depolarized by a depolarizer 14. An electronic circuit 18, preferably manufactured directed on the printed circuit board of backplane 7 of DG. 1, controls modulator 16 and may provide power to laser 12. Input data 19 is fed to the controller 18, which then controls modulator 16 to modulate the light from laser 12 in reflective of the input data 19.

The transceiver of the present invention preferably operates a phase-modulated mode through conventional amplitude-modulated transmitters and receivers, including those using return-to-zero type signals, for example, may also be used. The phase-modulated signals have the advantage that breach detection by the energy level detector work more effectively, since the amplitude of the optical signal is constant and thus a drop in the optical signal level is more easily detected.

Optical signals are received at connector 100 from fiber 111.

Receiver 11 includes two coupler splitters 31 and 131, each functioning as a splitter. Splitter 131 is preferably a wavelength division multiplexed coupler splitter to allow the OTDR 132 to operate at one optical wavelength, for example 1570 nm, while the transmitter/receiver system 19 and received data (energy) 34 are carried on a different wavelength, for example 1550 nm. The transceiver system 19 and the OTDR 132 in transceiver card 1 to be communicated transmissively operate without interruption or corruption of the received data stream 34. Splitter 131 splits off the wavelength of light applicable to the OTDR 132 fiber 133, which then is input to OTDR 132. Splitter 31 then splits off a portion of the remaining other light, directing part of that optical energy to an

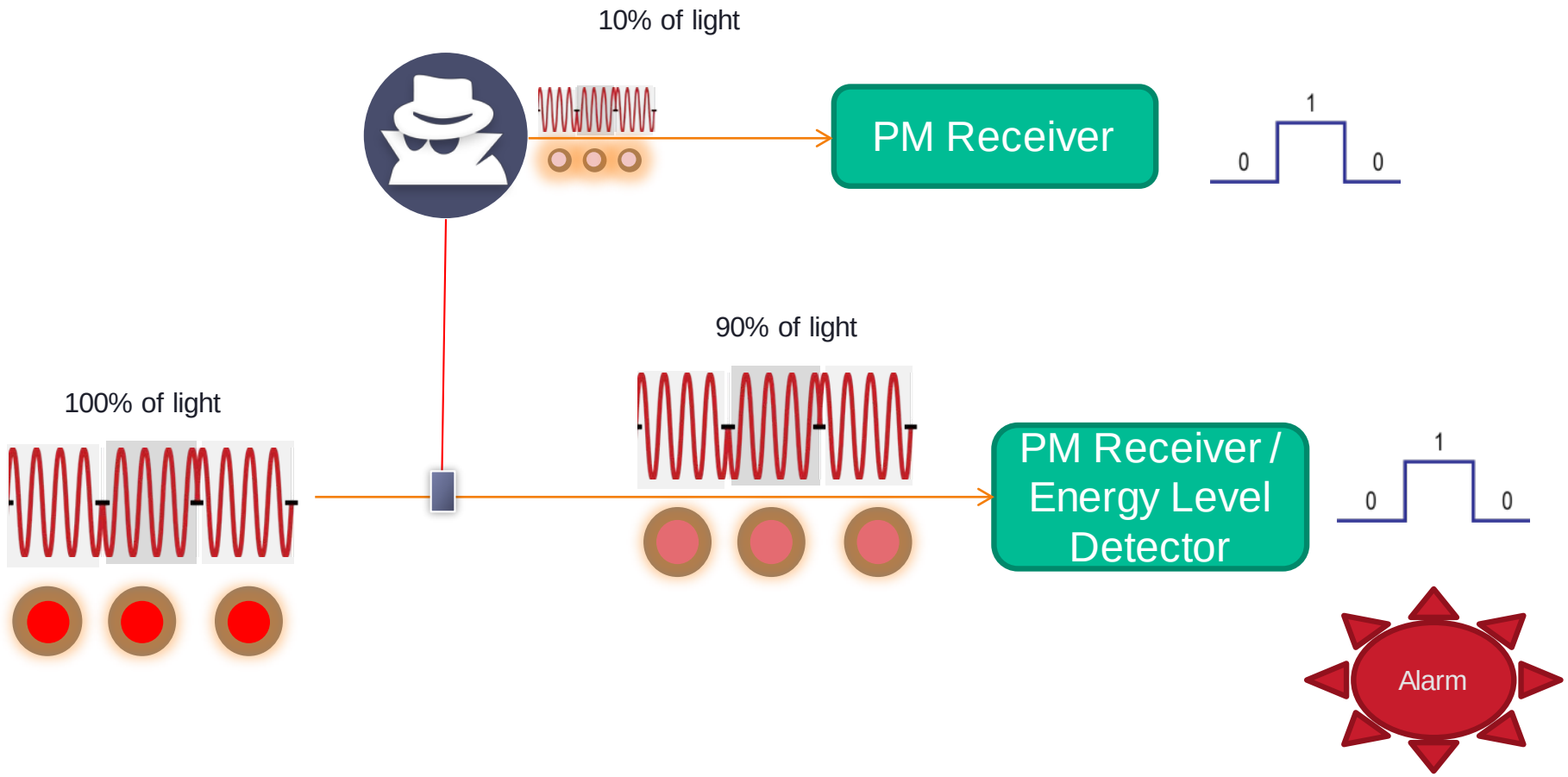
used. The phase-modulated signals have the advantage that breach detection by the energy level detector work more effectively, since the amplitude of the optical signal is constant and thus a drop in the optical signal level is more easily detected.

’898 patent at 4:48-52

- The patent explains that the amplitude of a phase modulated signal is **constant**.
- The patent explains that the **constant amplitude** of the received phase modulated signal makes it easier to detect changes in amplitude than detecting changes in an amplitude modulated signal.

’898 patent at 4:48-52

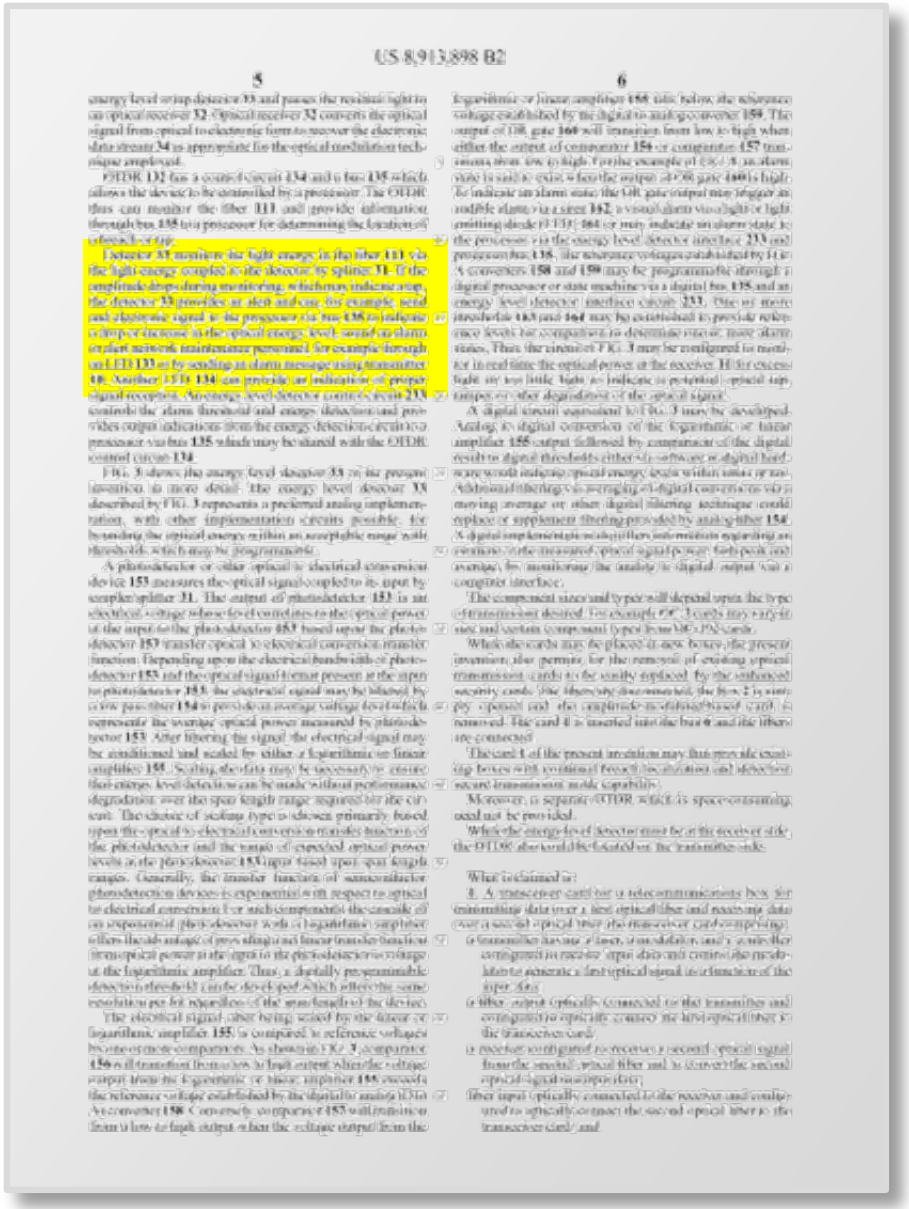
Solution As Explained by The Patent: Detect Tapping by Observing Changes in The Energy Level of a Phase Modulated (PM) Signal Using An Energy Level Detector



The phase-modulated signals have the advantage that breach detection by the energy level detector work more effectively, since the amplitude of the optical signal is constant and thus a drop in the optical signal level is more easily detected. 4:43-47

With Oyster's patented technology an alarm occurs when the change in the received light energy exceeds a threshold.

If A Drop Was Detected, Then An Alert Was Provided



US 8,913,898 B2

5 6

Detector **33** monitors the light energy in the fiber **111** via the light energy coupled to the detector by splitter **31**. If the amplitude drops during monitoring, which may indicate a tap, the detector **33** provides an alert and can, for example, send and electronic signal to the processor via bus **135** to indicate a drop or increase in the optical energy level, sound an alarm or alert network maintenance personnel, for example through an LED **133** or by sending an alarm message using transmitter **10**. Another LED **134** can provide an indication of proper

’898 patent at 5:11-19

- If the received signal amplitude (i.e., energy) drops during monitoring, which may indicate a tap, the detector provides an alert.

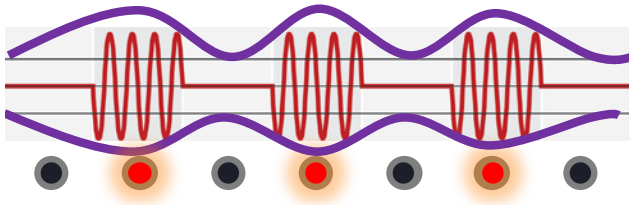
’898 patent at 5:11-19

Oyster's Solution: Monitor Changes in Light Energy (Intensity / Brightness)

Signal envelope (~ energy / amplitude)

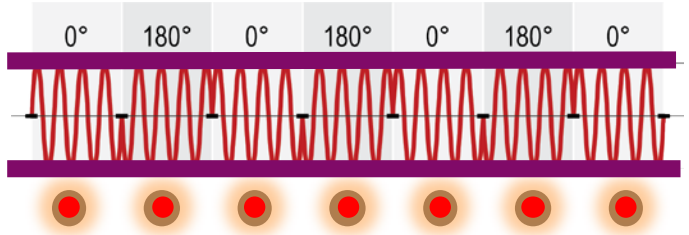
Modulated Optical Signal

AMPLITUDE MODULATED OPTICAL SIGNAL



The intensity (brightness) of an amplitude modulated signal is ***not constant***

PHASE MODULATED OPTICAL SIGNAL



The intensity (brightness) of an ideal phase modulated signal is ***constant***

used. The phase-modulated signals have the advantage that breach detection by the energy level detector work more effectively, since the amplitude of the optical signal is constant and thus a drop in the optical signal level is more easily detected.

'898 patent at 4:48-52

HOW DOES THE ENERGY LEVEL DETECTOR DISCLOSED IN THE ASSERTED PATENTS WORK?

Energy Level Detector # 33

Transceiver

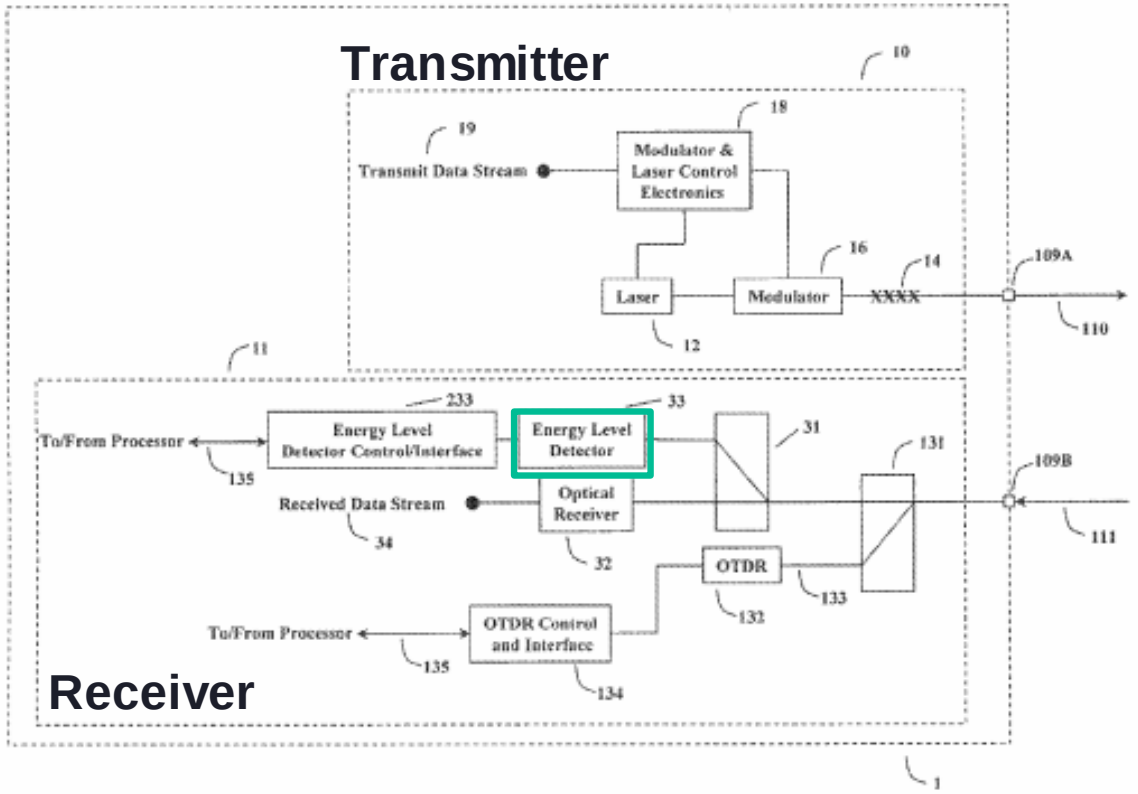


Figure 2

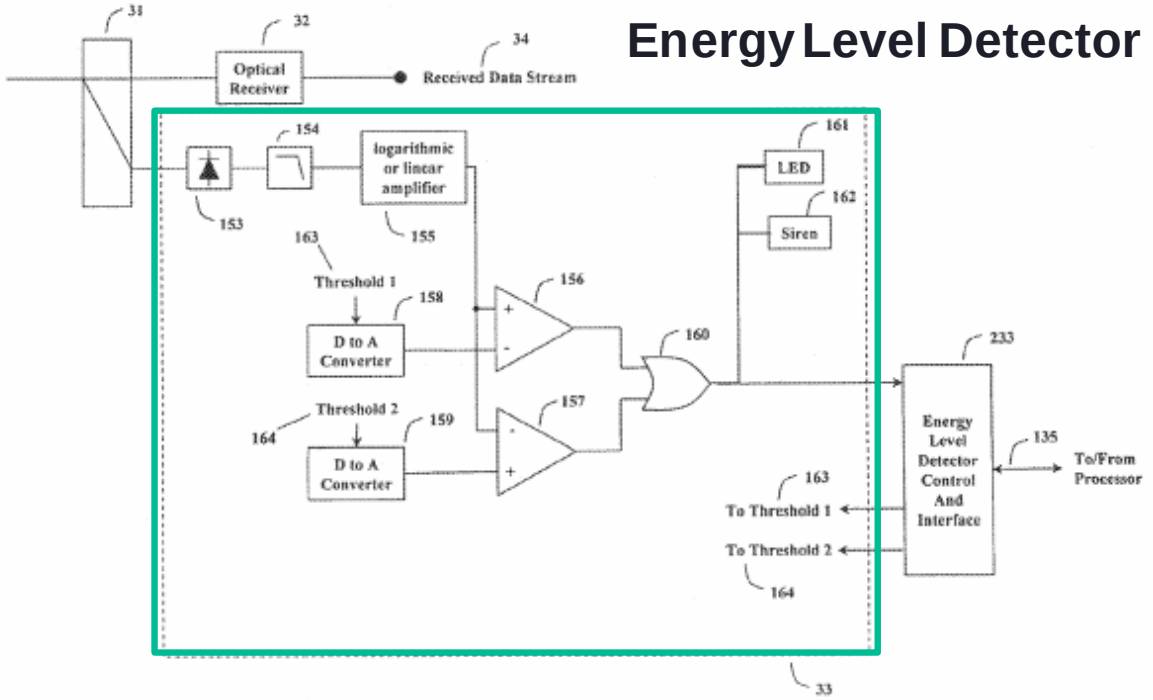


Figure 3

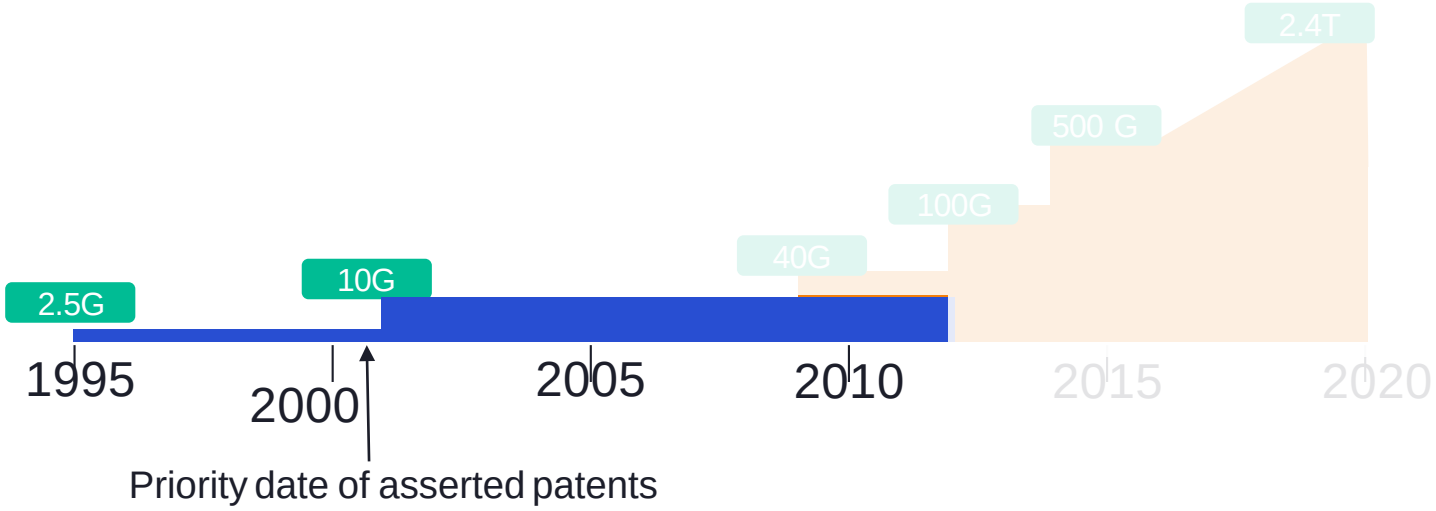
In the energy level detector, the output of photodetector 153 is an electrical voltage that is correlated with the optical power at the input to the photodetector.

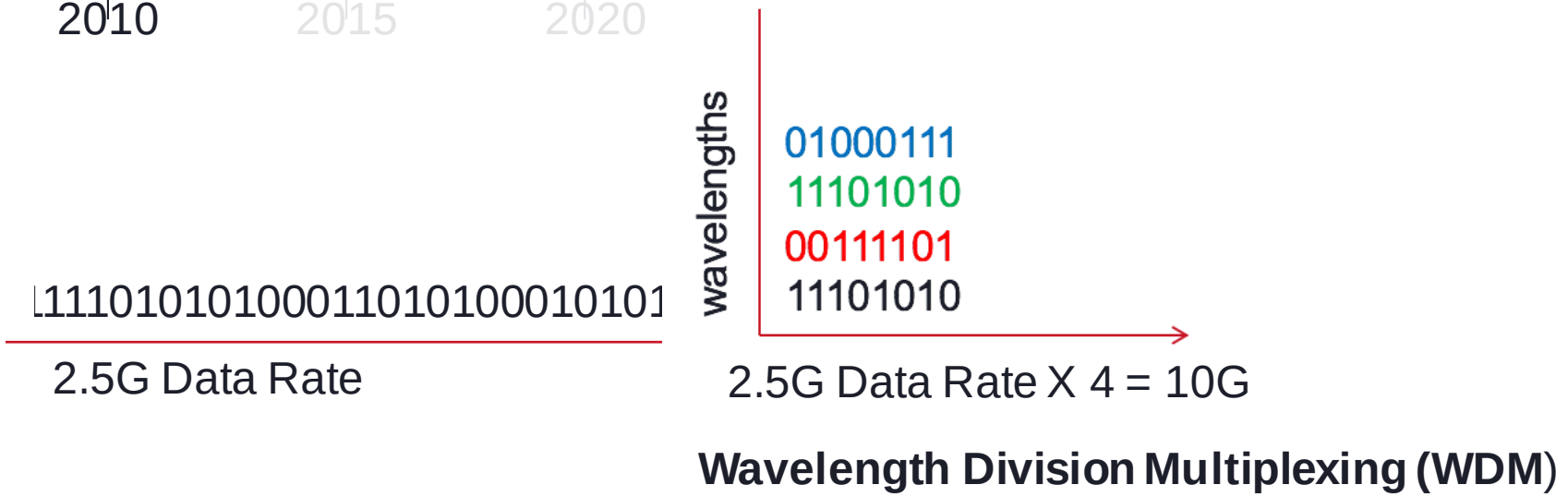
The electrical signal, may be averaged, and is compared to reference voltages that correspond to upper and lower thresholds that cannot be crossed without setting off an alarm.

Major Technology Progress Over The Last 20 Years Since Oyster's Patents Were Filed.

Wavelength Division Multiplexing Coherent Optics: Gb/s → Tb/s

Even with Continuous Improvements (WDM) Direct Detection Systems Start to Lose Relevance In Early 2010's



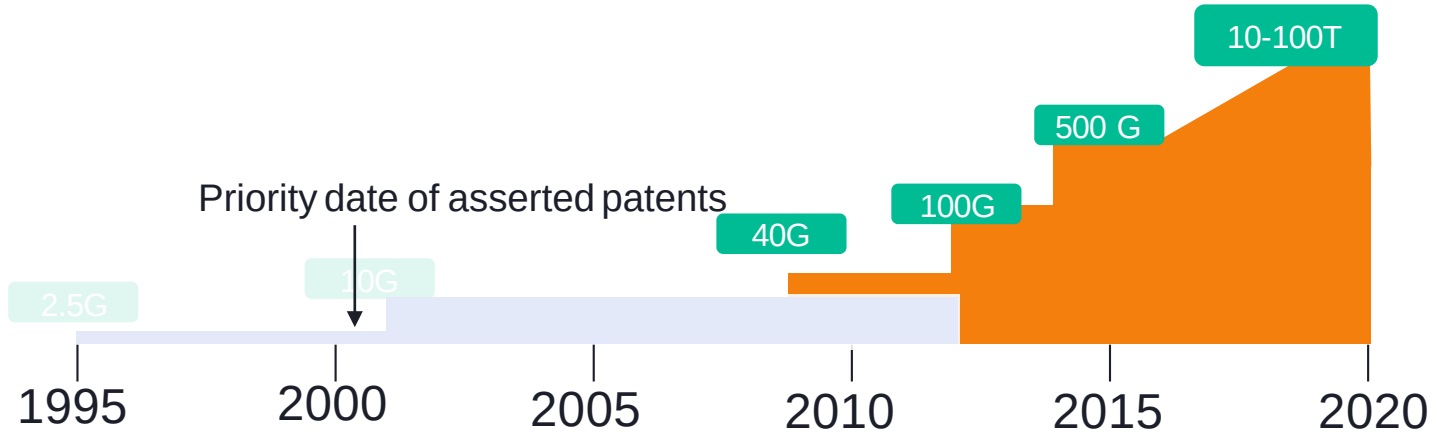


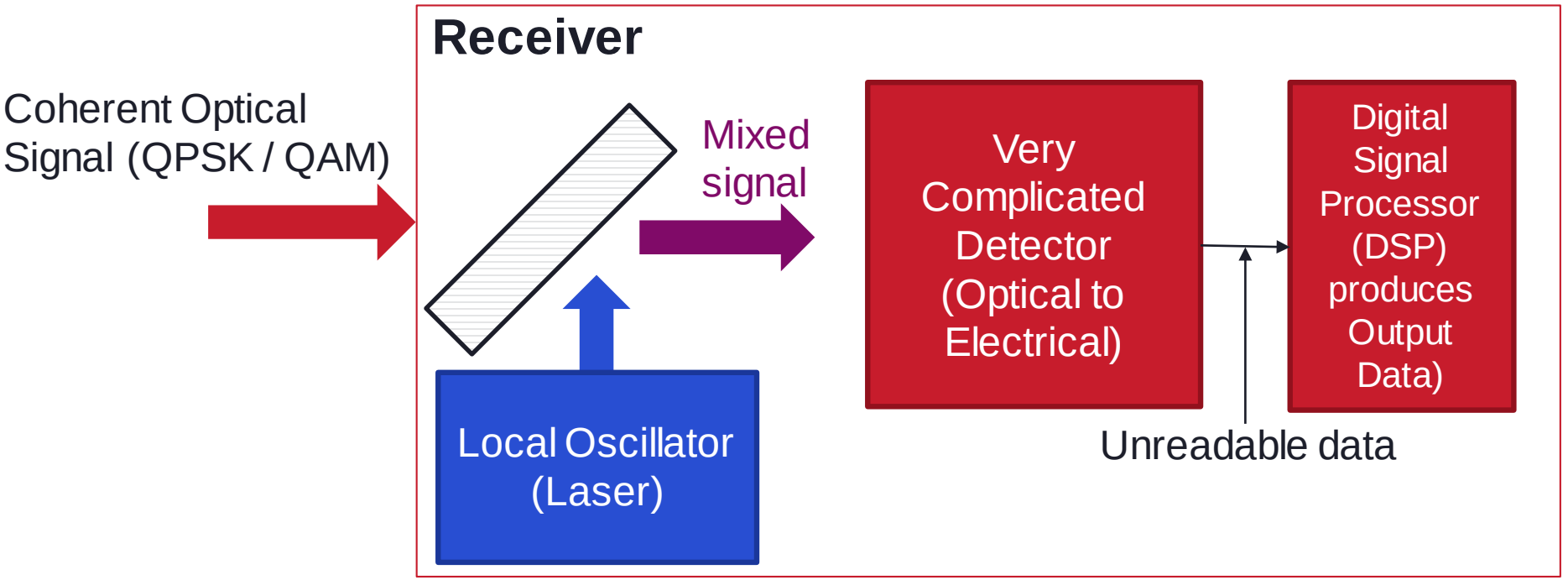
Wavelength Division Multiplexing (WDM)

G denotes gigabits (billion) per second

Coherent Optical Communications: Novel Technology that Took Over a Decade to Design

- Signal phase, amplitude, and polarization modulated.
- Receiver mixes the optical signal with a specially tuned laser and powerful DSP
- Integrate coherent system with WDM
- Enables Terabit/sec communications



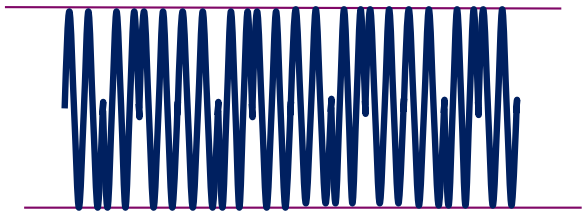


Output data

Energy Level Detection And Signal Type

Envelope

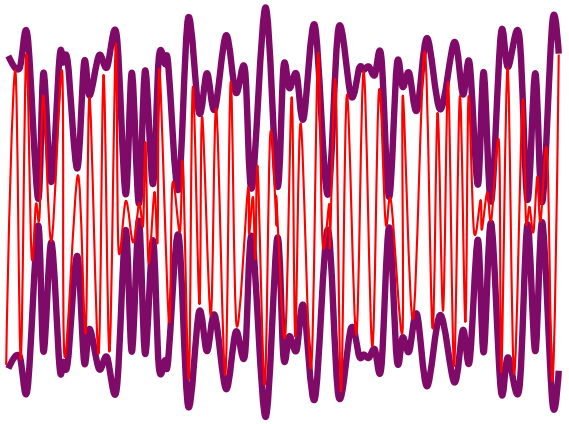
Phase Modulated Signal



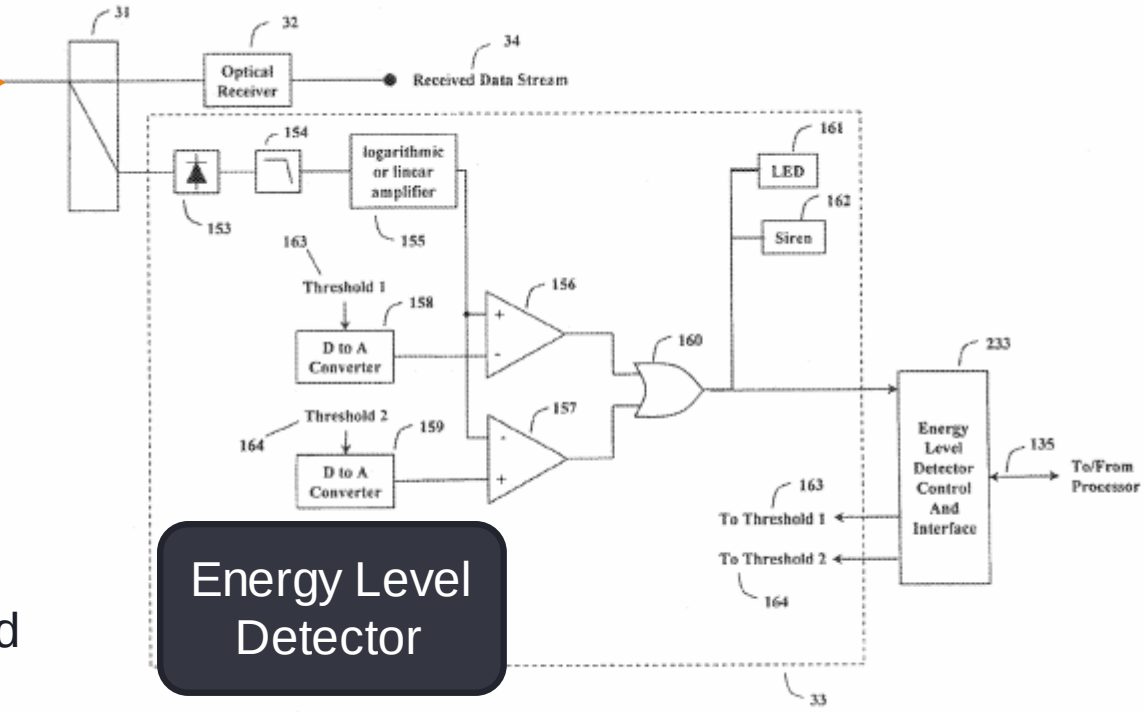
Oyster's Energy Level Is Designed for Constant Envelope Phase Modulation with Direct Detection Receivers.

Envelope

Coherent Optical Signal



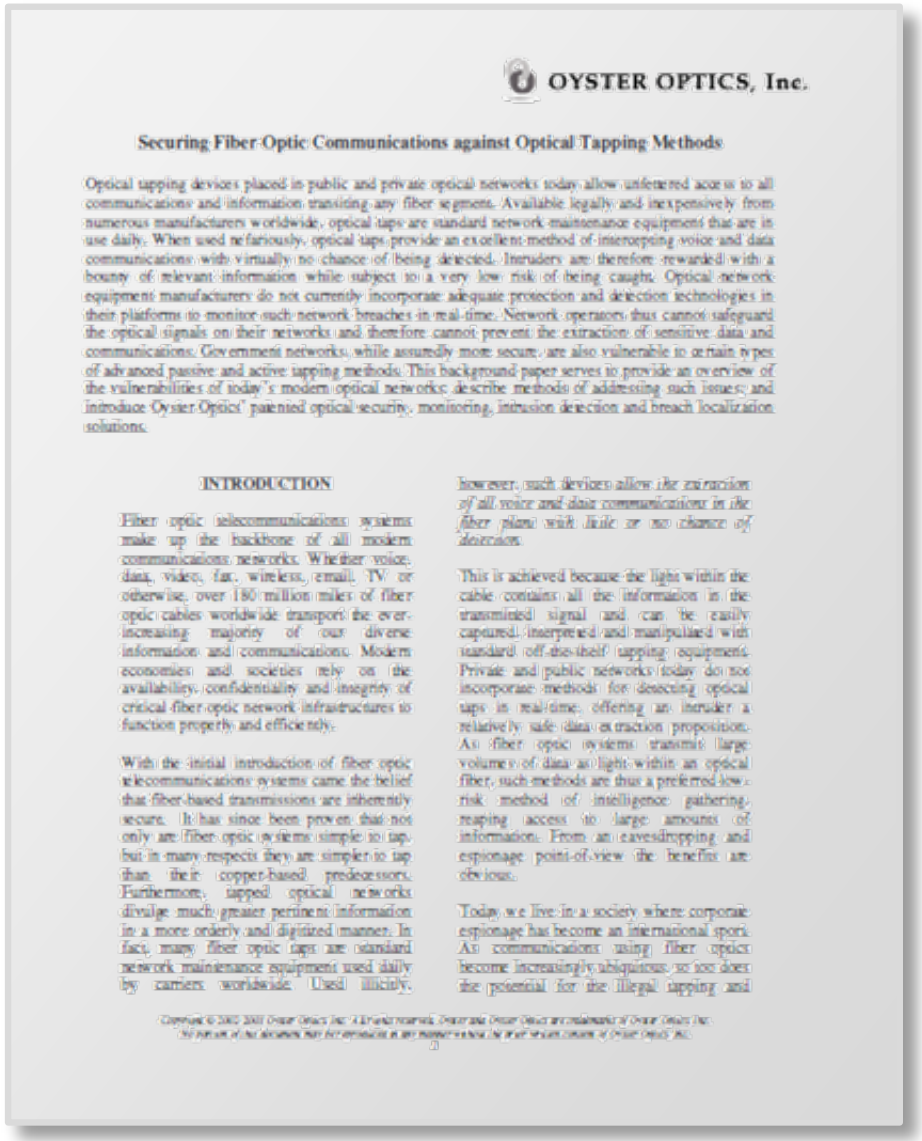
Oyster's Energy Level Detector And Receiver Are Not Designed For Extremely Complex Coherent Signals with Peaky, Variable envelopes.



Energy Level Detector

Figure 3

Oyster's Described Advantage of Patented Phase-Modulated Signals



OYSTER OPTICS, Inc.

Securing Fiber Optic Communications against Optical Tapping Methods

Optical tapping devices placed in public and private optical networks today allow unfettered access to all communications and information transiting any fiber segments. Available legally and inexpensively from numerous manufacturers worldwide, optical taps are standard network maintenance equipments that are in use daily. When used nefariously, optical taps provide an excellent method of intercepting voice and data communications with virtually no chance of being detected. Intruders are therefore rewarded with a bounty of relevant information while subject to a very low risk of being caught. Optical network equipment manufacturers do not currently incorporate adequate protection and detection technologies in their platforms to monitor such network breaches in real-time. Network operators thus cannot safeguard the optical signals on their networks and therefore cannot prevent the extraction of sensitive data and communications. Government networks, while assumedly more secure, are also vulnerable to certain types of advanced passive and active tapping methods. This background paper serves to provide an overview of the vulnerabilities of today's modern optical networks, describe methods of addressing such issues, and introduce Oyster Optics' patented optical security, monitoring, intrusion detection and breach localization solutions.

INTRODUCTION

Fiber optic telecommunications systems make up the backbone of all modern communications networks. Whether voice, data, video, fax, wireless, email, TV or otherwise, over 180 million miles of fiber optic cables worldwide transport the ever-increasing majority of our diverse information and communications. Modern economies and societies rely on the availability, confidentiality and integrity of critical fiber optic network infrastructures to function properly and efficiently.

With the initial introduction of fiber optic telecommunications systems came the belief that fiber-based transmissions are inherently secure. It has since been proven that not only are fiber optic systems simple to tap, but in many respects they are simpler to tap than their copper-based predecessors. Furthermore, tapped optical networks divulge much greater pertinent information in a more orderly and digitized manner. In fact, many fiber optic taps are standard network maintenance equipment used daily by carriers worldwide. Used illicitly, however, such devices *allow the extraction of all voice and data communications in the fiber plant with little or no chance of detection.*

This is achieved because the light within the cable contains all the information in the transmitted signal and can be easily captured, interpreted and manipulated with standard off-the-shelf tapping equipments. Private and public networks today do not incorporate methods for detecting optical taps in real-time, offering an intruder a relatively safe data extraction proposition. As fiber optic systems transmit large volumes of data as light within an optical fiber, such methods are thus a preferred low-risk method of intelligence gathering, reaping access to large amounts of information. From an eavesdropping and espionage point-of-view the benefits are obvious.

Today we live in a society where corporate espionage has become an international sport. As communications using fiber optics become increasingly ubiquitous, so too does the potential for the illegal tapping and

Dkt. No. 100-3; Ex. M (Oyster Optics White Paper)

Even though the input and output electronic data streams to the multiplexors and switches remain the same, the light transmitting the data is in a patented secure phase modulated format different from any commercially available products. Because of the format of the light, Oyster Optics' technologies are therefore able to provide an extremely precise and sensitive tap detection system, which would not function with existing common equipment utilizing insecure amplitude or intensity modulated signals. Furthermore, Oyster Optics integrates an Optical Time Domain Reflectometer ("OTDR") to instantaneously locate the exact source of an intrusion or maintenance event and determine its origins, such as an actual tap, a physical line break, or even simple fiber degradation.

Dkt. No. 100-3; Ex. M at 14